
HBCI

Homebanking-Computer-Interface

- Schnittstellenspezifikation -

Herausgeber:

Bundesverband deutscher Banken e.V., Köln

Deutscher Sparkassen- und Giroverband e.V., Bonn

Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V., Bonn

Bundesverband Öffentlicher Banken Deutschlands e.V., Bonn

Version: 2.0.1

Stand: 02.02.1998

Die vorliegende Schnittstellenspezifikation für eine automatisiert nutzbare multibankfähige Homebanking-Schnittstelle (im folgenden: Schnittstellenspezifikation) wurde im Auftrag des Zentralen Kreditausschusses entwickelt. Sie wird hiermit zur Implementation in Kunden- und Kreditinstitutssysteme freigegeben.

Die Schnittstellenspezifikation ist urheberrechtlich geschützt. Zur Implementation in Kunden- und Kreditinstitutssysteme wird interessierten Herstellern unentgeltlich ein einfaches Nutzungsrecht eingeräumt. Im Rahmen des genannten Zwecks darf die Schnittstellenspezifikation auch - in unveränderter Form - vervielfältigt und zu den nachstehenden Bedingungen verbreitet werden.

Umgestaltungen, Bearbeitungen, Übersetzungen und jegliche Änderung der Schnittstellenspezifikation sind untersagt. Kennzeichnungen, Copyright-Vermerke und Eigentumsangaben dürfen in keinem Falls geändert werden.




Im Hinblick auf die Unentgeltlichkeit des eingeräumten Nutzungsrechts wird keinerlei Gewährleistung oder Haftung für Fehler der Schnittstellenspezifikation oder die ordnungsgemäße Funktion der auf ihr beruhenden Produkte übernommen. Die Hersteller sind aufgefordert, Fehler oder Auslegungsspielräume der Spezifikation, die die ordnungsgemäße Funktion oder Multibankfähigkeit von Kundenprodukten behindern, dem Zentralen Kreditausschuß zu melden. Es wird weiterhin ausdrücklich darauf hingewiesen, daß Änderungen der Schnittstellenspezifikation durch den Zentralen Kreditausschuß jederzeit und ohne vorherige Ankündigung möglich sind.

Eine Weitergabe der Schnittstellenspezifikation durch den Hersteller an Dritte darf nur unentgeltlich, in unveränderter Form und zu den vorstehenden Bedingungen erfolgen.

Dieses Dokument kann abgerufen werden unter <http://www.siz.de/siz/hbci/hbcispec.html>

Versionsführung

Das vorliegende Dokument wurde von folgenden Personen erstellt bzw. geändert:

Name	Organisation	Datum	Version	Dokument	Anmerkungen
Stein	 IZ	22.11.1996	1.0	hbc10.doc	Erste vom ZKA verabschiedete Version
Stein	 IZ	24.07.1997	2.0	hbc120a.doc hbc120b.doc hbc120c.doc hbc120d.doc	Änderungen und Fehlerkorrekturen sowie neue Geschäftsvorfälle
Stein	 IZ	02.02.1998	2.0.1	hbc1201a.doc hbc1201b.doc hbc1201c.doc hbc1201d.doc	Änderungen und Fehlerkorrekturen zur Version 2.0

Änderungen gegenüber der Version 2.0:

Änderungen sind im Dokument durch einen Randbalken markiert. Falls sich die Kapitelnumerierung geändert hat, bezieht sich die Kapitelangabe auf die neue Nummerierung.

lfd. Nr.	Kapitel	Kapitelnummer	CR ¹	Art ²	Beschreibung
1	Einleitung	I.	D22	E	Angabe der für die einzelnen Verbände reservierten Segmentkennungen
2				E	Weitere Aussagen über die Vergabe der Kennungen hinzugefügt.
3	Nachrichtenaufbau	II.4.2	D33	K	Klarstellung, daß nur binäre Daten im Byteformat über HBCI transportiert werden können.
4		II.5.3		K	Bei den mehrfach verwendeten Elementen wurden wie bei anderen Strukturen jeweils Name, Typ und Kennung angegeben.
5		II.6.2	D29	Ä	Festlegung, daß das DE „HBCI-Version“ immer der Version des HBCI-Dokuments entspricht (Beispiel angepaßt).
6		II.7.1	D30	Ä	Die Segmente HNSHK und HNSHA können 1-3 mal auftreten.
7			D20	Ä	Segmentfolge „Aufträge“ als Menge aller Auftragssegmente definiert, um die Kundennachricht korrekt abbilden zu können.
8		II.7.2		E	Segmentfolge „Aufträge“ dokumentiert
9		II.8.1	D44	K	Beschreibung, welche Signatur-ID für Kreditinstitutsnachrichten zu verwenden ist.
10			D20	Ä	Segmentfolge „Datensegmente“ als Menge aller Datensegmente definiert, um die Kreditinstitutsnachricht korrekt abbilden zu können.
11		II.8.2	D21	K	Im Segment HIRMG darf nur dann ein Erfolgscode eingestellt werden, wenn alle Aufträge fehlerfrei sind.
12		II.8.4		K	Beschreibung korrigiert
13			D20	K	Formatbeschreibung modifiziert
14				K	Segmentfolge „Datensegmente“ erläutert; Beispiel überarbeitet
15		II.8.5.3 II.8.5.4.3	D23	E	Vorliegen eines 'unbekannten Aufbaus' wurde definiert. Rückmeldungscode 9110 „Unbekannter Aufbau hinzugefügt“
16		II.8.5.4	D45	E	Rückmeldungscode 9050 „Teilweise fehlerhaft“ und 3060 „Teilweise liegen Warnungen/Hinweise vor“ hinzugefügt.
17		II.9	D10	Ä	Das Kap. „Nachrichtenaufbau bei Verschlüsselung“ wurde verschoben, da es sowohl für Kunden als auch für Kreditinsti-

¹ Die Spalte 'CR' dient nur der internen Zuordnung von Änderungsanträgen.

² F = Fehler; Ä = Änderung; K = Klarstellung; E = Erweiterung

lfd. Nr.	Kapitel	Kapitel-nummer	CR ¹	Art ²	Beschreibung
18			D20	Ä	tutsnachrichten gilt. Nachricht „Kundennachricht verschlüsselt“ wurde umbenannt in „Verschlüsselte Nachricht“, da sie sowohl für Kunden- als auch für Kreditinstitutsnachrichten gilt.
19	Dialogspezifikation	III.3		K	Aufzählung des Zwecks der Dialoginitialisierung überarbeitet
20		III.3.1.1		Ä	Segment „Synchronisierung“ aus Dialoginitialisierung gelöscht (nach III.8 verschoben).
21		III.3.1.3	D8	F	Die Segmentversion des Segments „Verarbeitungsvorbereitung“ war fälschlich auf 1 gesetzt und wurde auf den Wert '2' geändert.
22		III.3.2.1		Ä	Segment „Synchronisierungsantwort“ aus Dialoginitialisierungsantwort gelöscht (nach III.8 verschoben).
23		III.3.2.5		K	Ausdruck „beliebiger Länge“ gelöscht, da max. 2048 Byte zugelassen sind.
24		III.5.1	D20	Ä	Name der Kreditinstitutsnachricht geändert
25		III.5.2	D20	Ä	Segmentfolge „Aufträge“ als Menge aller Auftragssegmente definiert, um die Kundennachricht korrekt abbilden zu können.
26				F	Die Aussage, daß keine Datensegmente zurückgemeldet werden, ist falsch.
27		III.5.3	D20	Ä	Name der Nachricht geändert
28		III.7		Ä	DEG „Statusmeldung“ in „Rückmeldung“ umbenannt.
29				F	Numerierung der Des im Segment HIPRO korrigiert
30		III.8		K	Synchronisierung wird jetzt als eigener Nachrichtentyp in Kap. III.8 beschrieben (neue Formate und Formatbeschreibungen hinzugefügt).
31			D25	K	Bei der Synchronisierung der Signatur-ID ist immer der höchste bisher eingereichte Wert zurückzumelden.
32			D26	K	Im Fall der Synchronisierung der Signatur-ID ist für die Signaturbildung als Signatur-ID ein festgelegter Wert zu verwenden.
33					'Signaturzähler' in 'Signatur-ID' umbenannt
34		III.8.2.2	D35	Ä	Format des DE „Sicherheitsreferenznummer“ wurde in num..16 geändert (Segmentversion wurde inkrementiert).
35	Bankparameterdaten	IV.1		F	Segmentname in „Kommunikationszugang rückmelden“ korrigiert.
36			D20	Ä	Segmentfolge „Parameterdaten“ als Menge aller Parametersegmente definiert, um die BPD korrekt abbilden zu können.
37		IV.4	D37	Ä	DE „Mischung zulässig“ eingefügt, um angeben zu können, ob Sicherheitsverfahren gemischt werden können (Segmentversion inkrementiert, Beispiel angepaßt).

Ifd. Nr.	Kapitel	Kapitelnummer	CR ¹	Art ²	Beschreibung
38		IV.6	D27	K	Hinweis, daß institutsindividuell entweder alle oder nur die im aktuellen Dialog gültigen Segmentversionen in die BPD eingestellt werden können.
39			D30	K	Belegung des Feldes „Anzahl Signaturen mindestens“ wurde genauer erläutert.
40		IV.7		E	Kapitel zur Erläuterung der Segmentfolge „Parameterdaten“ eingefügt.
41	Userparameterdaten	V.1		F	Segmentname in „Kontoinformation“ geändert
42		V.3	B34	Ä	Status des DE „Kontowährung“ wurde auf „Kann“ geändert; Erläuterung zum DE „Kontowährung“ geändert (Segmentversion daher auf 3 geändert).
43			L7	Ä	Die Restriktion '>0' bei der GDG „Limitbetrag“ (2 x) wurde entfernt, da diese bei DEGs nicht erlaubt ist.
44	Sicherheit	VI.2.1.2	D9	K	Erläuterung bzgl. der Signaturbildung nach ISO 9796 hinzugefügt.
45		VI.2.2	D43	K	Hinweis hinzugefügt, daß der Nachrichtenschlüssel dynamisch generiert werden muß.
46			D39	K	Die Bitnumerierung in den Abbildungen 13-17 wurde korrigiert.
47		VI.2.3		E	Herstellerhinweis ergänzt
48		VI.3.1.3.1	L12	K	Erläuterung zum Ausdruck „großer Primteiler“ hinzugefügt.
49		VI.3.1.3.2		K	Inhalt des Ini-Briefs wurde genauer erläutert
50			L6	K	Exponent, Modulus und Hashwert des Beispiels im Ini-Brief wurden in „echte“ Werte geändert.
51		VI.3.1.3.3	D38	K	Klarstellung, daß bei einer Schlüsseländerung des Kunden der neue Schlüssel 'ab sofort' gilt.
52		VI.4	D30	K	Klarstellung, daß alle Kundennachrichten zu signieren sind.
53			B31	K	Die Vorgehensweise bei der Verifikation von mehreren Signaturen ist kreditinstitutspezifisch.
54		VI.5.1.3		K	Erläuterung zum DE „Identifizierung der Partei“ überarbeitet.
55		VI.5.2.1	D35	Ä	Format des DE „Sicherheitsreferenznummer“ wurde in num..16 geändert (Segmentversion wurde inkrementiert, Beispiel angepaßt).
56		VI.5.2.2		E	Beispiele hinzugefügt
57		VI.5.2.3		E	Beispiele hinzugefügt
58		VI.5.4.1		E	Beispiele hinzugefügt
59		VI.5.4.2		E	Beispiele hinzugefügt
60		VI.6.1.1		Ä	Segment in „Schlüsseländerung“ umbenannt.
		VI.6.1.2	D32	Ä	Zur Referenzierung bei nicht vorliegendem Schlüssel ist der Wert '999' zu verwenden.
		VI.6.1.4	B17	K	In die DEG 'Schlüsselname' sind bei Sperrung beider Schlüssels immer die Merk-
		VI.6.1.5			

lfd. Nr.	Kapitel	Kapitel-nummer	CR ¹	Art ²	Beschreibung
61					male des Signierschlüssels einzustellen.
		VI.6.1.5	B17	Ä	Beispiel geändert: Auf den Signierschlüssel wird nicht mit „B“ (für beide), sondern muß mit „S“ referenziert werden.
62		VI.6.2.2		Ä	Kapitel- und Formatname geändert
63			D36	K	Es wurde klargestellt, daß vom Kunden immer beide Schlüssel anzufordern sind.
64		VI.6.2.3		Ä	Kapitel- und Formatname geändert
65		VI.6.2.4	D32	Ä	Belegung der DEG „Schlüsselname“ bei unsignierter Sperrung definiert.
66			B17	Ä	Bei der Sperrung sind die Identifikationsmerkmale des Signierschlüssels einzustellen. Auf diesen kann nicht „B“ (für beide), sondern muß mit „S“ referenziert werden.
67	Geschäftsvorfälle	VII.1.1.1	L7	Ä	Die Restriktion '>0' bei der DEG „Betrag“ wurde entfernt, da diese bei DEG's nicht erlaubt ist.
68			D20	Ä	Parametersegment eindeutig benannt
69				F	Beispiel zum Parametersegment korrigiert.
70		VII.1.1.3.1	B29	Ä	Der minimale Wert für das DE „Minimale Vorlaufzeit“ wurde auf 0 geändert (Segmentversionen daher inkrementiert).
71			D20	Ä	Parametersegment eindeutig benannt
72				F	Beispiele korrigiert
73		VII.1.1.3.2	B29	Ä	Der minimale Wert für das DE „Minimale Vorlaufzeit“ wurde auf 0 geändert (Segmentversionen daher inkrementiert).
74			D16	Ä	Die BPD-Parameter der Einreichung und Änderung von terminierten Überweisungen wurde angeglichen (Segmentversionen daher inkrementiert).
75			D20	Ä	Parametersegment eindeutig benannt
76				F	Beispiele korrigiert
77		VII.1.1.3.3	D20	Ä	Parametersegment eindeutig benannt
78				F	Beispiel zum Parametersegment korrigiert.
79		VII.1.1.3.4	B26	K	Klarstellung, daß das aktuell gültige Ausführungsdatum einzustellen ist.
80				F	Beispiele korrigiert
81		VII.1.1.4.1	B29	Ä	Der minimale Wert für das DE „Minimale Vorlaufzeit“ wurde auf 0 geändert (Segmentversionen daher inkrementiert).
82			D20	Ä	Parametersegment eindeutig benannt
83				F	Beispiele korrigiert
84		VII.1.1.4.2	D16	Ä	Die BPD-Parameter der Einreichung und Änderung von Daueraufträgen wurde angeglichen (Segmentversionen daher inkrementiert).
85			D20	Ä	Parametersegment eindeutig benannt
86				F	Beispiele korrigiert
87		VII.1.1.4.3	D20	Ä	Parametersegment eindeutig benannt
88				F	Beispiele korrigiert
89		VII.1.1.4.4		F	Beispiele korrigiert

lfd. Nr.	Kapitel	Kapitelnummer	CR ¹	Art ²	Beschreibung
90		VII.1.1.4.5	B21 B27	K	Begriffe „Änderungs-“, und „Aussetzungstermine“ erläutert; Herstellerhinweis ergänzt.
91				F	Beispiele korrigiert
92		VII.1.1.4.6	D20	Ä	Parametersegment eindeutig benannt
93				F	Beispiele korrigiert
94		VII.1.1.5	D20	Ä	Parametersegment eindeutig benannt
95				F	Beispiel zum Parametersegment korrigiert
96		VII.1.2.1	D20	Ä	Parametersegment eindeutig benannt
97				F	Beispiel zum Parametersegment korrigiert
98		VII.1.2.2		E	Beispiele für RückmeldungsCodes hinzugefügt.
99			D20	Ä	Parametersegment eindeutig benannt
100				F	Beispiel zum Parametersegment korrigiert
101		VII.2.1		K	Verweis auf DFÜ-Abkommen entfernt.
102				E	Es werden das alte und das neue Format MT 940 und MT 942 unterstützt. Die Unterscheidung erfolgt anhand der Segmentversionen.
103		VII.2.1.1		Ä	DE „Kontowährung“ in Segment HKKAN eingefügt (Segmentversionen daher inkrementiert; Beispiel angepaßt).
104			D20	Ä	Parametersegment eindeutig benannt
105				F	Beispiel zum Segment HIKAZS korrigiert
106		VII.2.1.2	D34	K	Festlegung, daß als Basis für die Bestimmung neuer Umsätze der letzte Umsatzabruf über HBCI herangezogen wird.
107				Ä	DE „Kontowährung“ in Segment HKKAZ eingefügt (Segmentversionen daher inkrementiert; Beispiel angepaßt).
108			D20	Ä	Parametersegment eindeutig benannt
109				F	Beispiel zum Segment HIKANS korrigiert.
110		VII.2.2	B35	Ä	Neues DE „Kontowährung“ in Segmenten HKSAL und HISAL eingefügt (Segmentversionen daher inkrementiert).
111				F	Beispiele korrigiert
112		VII.3	B33	K	Welches Konto zur Berechtigungsprüfung herangezogen wird, kann kreditinstitutsindividuell entschieden werden.
113			B33	Ä	Einfügung des DE „Kontraktreferenz“ in das Format „Festgeld“.
114			B33	K	Einschränkung, daß das Belastungskonto bei demselben Institut geführt werden muß.
115			B32	K	Erläuterung, daß die Laufzeit einer Festgeldanlage mit der Zinsmethode korrespondieren muß.
116		VII.3.1	D20	Ä	Parametersegment eindeutig benannt
117				F	Beispiel zum Segment HIFGKS korrigiert
118		VII.3.2	B33	Ä	Einfügung des DE „Kontraktreferenz“ in die Segmente HKFGN und HIFGN (Segmentversionen daher inkrementiert).
119			D20	Ä	Parametersegment eindeutig benannt
120				F	Beispiele korrigiert

lfd. Nr.	Kapitel	Kapitelnummer	CR ¹	Art ²	Beschreibung
121		VII.3.3	B33	Ä	Einfügung des DE „Kontraktreferenz“ in die Segmente HKFGA und HIFGA (Segmentversionen daher inkrementiert).
122			D20	Ä	Parametersegment eindeutig benannt
123				F	Beispiele korrigiert
124		VII.3.4	B33	Ä	Einfügung des DE „Kontraktreferenz“ in die Segmente HKFGP und HIFGP (Segmentversionen daher inkrementiert).
125				F	Beispiele korrigiert
126		VII.3.5	B33	Ä	Einfügung des DE „Kontraktreferenz“ in die Segmente HKFGB und HIFGB (Segmentversionen daher inkrementiert).
127				K	Erläuterung für den Fall hinzugefügt, daß keine Kontraktreferenz im Kundenauftrag angegeben wurde.
128				F	Beispiele korrigiert
129		VII.3.6	B33	Ä	Einfügung des DE „Kontraktreferenz“ in das Segment HKFGW (Segmentversionen daher inkrementiert).
130				E	Beispiel für Parametersegment hinzugefügt
131		VII.3.7	B33	Ä	Einfügung des DE „Kontraktreferenz“ in das Segment HKFPW (Segmentversionen daher inkrementiert).
132				E	Beispiel für Parametersegment hinzugefügt
133		VII.4.1	B36	E	DE „Eingabe Anzahl Einträge erlaubt“ in Parametersegment hinzugefügt (Segmentversionen daher inkrementiert).
134			D20	Ä	Parametersegment eindeutig benannt
135				Ä	Beispiele angepaßt
136		VII.5.1		E	Es werden das alte und das neue DTAZV-Format unterstützt. Die Unterscheidung erfolgt anhand der Segmentversionen.
137			B37	E	DE „Maximale Anzahl T-Sätze“ in Parametersegment hinzugefügt (Segmentversionen daher inkrementiert).
138			D20	Ä	Parametersegment eindeutig benannt
139				Ä	Beispiele angepaßt
140		VII.6.1.1	D20	Ä	Parametersegment eindeutig benannt
141				F	Beispiel zum Segment HIVDBS korrigiert
142		VII.7.1.1		Ä	DE „Kontowährung“ in Segment HKKDM eingefügt (Segmentversionen daher inkrementiert).
143			D20	Ä	Parametersegment eindeutig benannt
144				Ä	Beispiele angepaßt
145		VII.7.1.2	D20	Ä	Parametersegment eindeutig benannt
146				Ä	Beispiele angepaßt
147		VII.7.2.1		F	Beispiele korrigiert
148		VII.7.2.2		F	Beispiele korrigiert
149	Anlagen	VIII.1	D40	Ä	In der aktuellen HBCI-Version werden keine 'zusätzlich akzeptierten Segmentversionen' zugelassen. (Ausnahmen: Geschäftsvorfälle, bei denen mehrere Versionen eines Fremdformats zulässig sind: HKSUB,

Ifd. Nr.	Kapitel	Kapitelnummer	CR ¹	Art ²	Beschreibung
150					HKSLA, HKKAZ, HKKAN)
151				K	Geänderte Segmentversionen aktualisiert.
152		VIII.2	D19	E	Übersichtstabellen für Nachrichten, Segmentfolgen, Segmente, Datenelementgruppen und Datenelemente aufgenommen.
153		VIII.3		E	In der Übersicht des Nachrichtenaufbaus wurde bei jeder Nachricht eine ID angegeben, um auf die jeweiligen Nachrichten referenzieren zu können.
154		VIII.3.1	D30	Ä	Segmente HNSHK und HNSHA können im Kundenauftrag 1-3 mal auftreten.
155		VIII.5.1	D13	F	Fehler in den Beispielen wurden korrigiert.
156		VIII.6.1	D6	K	Hinweis hinzugefügt, daß es sich bei den Btx-FIF-Formaten nicht um HBCI-Formatbeschreibungen handelt.
157		VIII.6.1.3	D6	Ä	Format der BtxFIF-Längfelder wurde auf variable Länge (.8) geändert.
158		VIII.7	B19	K	Beim Abruf der Zugangsdaten werden keine Bank- oder Userparameterdaten zurückgemeldet.
159		VIII.8	D14	K	Einleitende Bemerkungen zum Kapitel „Chipapplikation“ hinzugefügt
160		VIII.8.2.7	L1	F	In der Beschreibung der Records des EF_BNK wurde das ASCII-Leerzeichen auf X'20' korrigiert.
161		VIII.9.2		Ä	Neues DTAZV-Format aufgenommen
162		VIII.9.3.1		K	Textkorrekturen durchgeführt
163		VIII.9.3.2 VIII.9.3.3		Ä	Euro-fähige Versionen der Formate MT 940 und MT 942 hinzugefügt.
		VIII.12		K	Literaturverzeichnis aktualisiert

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: 0
Kapitel: Inhaltsverzeichnis	Stand: 02.02.1998	Seite: 1

Inhaltsverzeichnis

Ein ausführliches Inhaltsverzeichnis befindet sich jeweils am Anfang jeden Kapitels.

- I. Einleitung
- II. Nachrichtenaufbau
- III. Dialogspezifikation
- IV. Bankparameterdaten (BPD)
- V. Userparameterdaten (UPD)
- VI. Sicherheit
- VII. Geschäftsvorfälle
- VIII. Anlagen

Kapitel: 0	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 2	Stand: 02.02.1998	Kapitel: Inhaltsverzeichnis

Abbildungsverzeichnis

Abb. 1: Übersicht der Schnittstellenbeziehungen

Abb. 2: Nachrichtenaufbau

Abb. 3: Logischer Nachrichtenaufbau

Abb. 4: Benutzer, mehreren Kunden zugeordnet

Abb. 5: Kunde, mehreren Benutzern zugeordnet

Abb. 6: Dialogabfolge

Abb. 7: Einzelbenutzer

Abb. 8: Mehrere Benutzer

Abb. 9: Verbindungsabbruch Fall 1

Abb. 10: Verbindungsabbruch Fall 2

Abb. 11: Verbindungsabbruch Fall 3

Abb. 12: Verbindungsabbruch Fall 4

Abb. 13: 2-Key-Triple-DES im CBC-Mode

Abb. 14: Verschlüsselung bei 2-Key-Triple-DES

Abb. 15: Entschlüsselung bei 2-Key-Triple-DES

Abb. 16: 2-Key-Triple-DES im ECB-Mode

Abb. 17: Verschlüsselung bei RSA (2-Key-Triple-DES)

Abb. 18: Beispiel für die Gestaltung des Ini-Briefs

Abb. 19: Lebenszyklus einer terminierten Überweisung

Abb. 20: Lebenszyklus Dauerauftrag

Abb. 21: Lebenszyklus Festgeld

Abb. 22: Aufbau der T-Online-Übergabeseite

Abb. 23: Datenelemente der Applikation „Banking“

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: 0
Kapitel: Inhaltsverzeichnis	Stand: 02.02.1998	Seite: 3

Abkürzungen

Abkürzung	Bedeutung
AC	Access Condition
AEF	Application Elementary File
AID	Application Identifier
BPD	Bankparameterdaten
BZÜ	Beleggebundenes Zahlscheinüberweisungsformular
CBC	Cipher Block Chaining
CID	Cardholders Information Data (Kartenidentifikationsdaten der ZKA-Chipkarte)
CLA	Class Byte
CR	Carriage-Return (Wagenrücklauf)
DDV	DES-DES-Verfahren
DE	Datenelement
DEG	Datenelementgruppe
DES	Data Encryption Standard
DF	Dedicated File
DFÜ	Synonym verwendet für "Datenkommunikation, die in Form von Filetransfer, E-Mail, Online-Nachrichtenaustausch etc. erfolgen kann"
DTA	s. DTAUS
DTAUS	Datensatzformat für den Inlandszahlungsverkehr (veröffentlicht in den Bedingungen für die Beteiligung von Kunden am beleglosen Datenträgeraustausch mittels Disketten)
DTAZV	Datensatzformat für den Auslandszahlungsverkehr
ECB	Electronic Code Book
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EF	Elementary File
EHKP	Einheitlich höhere Kommunikationsprotokolle
EU	Elektronische Unterschrift; basiert auf dem asymmetrischen RSA-Verfahren
EWU	Europäische Wirtschafts- und Währungsunion
FCI	File Control Information
FCP	File Control Parameters
FCS	Frame Check Sequence
FMD	File Management Data
GD	Gruppendatenelement
GDG	Gruppendatenelement-Gruppe
HBCI	Homebanking Computer Interface

Kapitel:	0	Version:	2.0.1	Homebanking-Computer-Interface (HBCI)
Seite:	4	Stand:	02.02.1998	Kapitel: Inhaltsverzeichnis

Abkürzung	Bedeutung
I	Information (z.B. Schlüsselart)
ID	Identifikationsmerkmal (Nummer oder alphanumerischer Code)
ISO	International Standards Organization
IV	Initialisierungsvektor
K	Datenstruktur ist optional (Kann)
KGK	Key Generating Key
LF	Line-Feed (neue Zeile)
M	Muß (Datenstruktur muß vorhanden sein und ist inhaltlich korrekt zu füllen)
MAC	Message Authentication Code; Symmetrisches Verfahren zur Erzeugung einer elektronischen Signatur (derzeit für die ZKA-Chipkarte eingesetzt)
MF	Master File
MFC	Multifunktions-Chipkarte
MIME	Multipurpose Internet Mail Extensions
MVE	Mehrfach verwendetes Element
N	Nachricht
PKD	Public-Key-Daten
RDH	RSA-DES-Hybridverfahren
RFC	Request for Comment
RSA	Asymmetrischer Algorithmus für die elektronische Unterschrift (EU) (vgl. MAC), benannt nach den Erfindern Rivest, Shamir und Adleman.
SEG	Segment
SEQ	Sequenznummer
SF	Segmentfolge
SFI	Short File Identifier
SSL	Secure Socket Layer
S.W.I.F.T.	Society for Worldwide Interbanking Financial Communication
T	Transaktion (z.B. Schlüsselart)
UN/EDIFACT	s. EDIFACT
UPD	Userparameterdaten
ZKA	Zentraler Kreditausschuß

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: 0
Kapitel: Inhaltsverzeichnis	Stand: 02.02.1998	Seite: 5

Definitionen

Begriff	Bedeutung
Abholauftrag	Synonym: Informationsauftrag. Ein →Auftrag an das Kreditinstitut, zur Bereitstellung und Übermittlung von Informationen (z.B. einen Kontoauszug), in Abgrenzung zu transaktionsrelevanten Aufträgen (z.B. Überweisungsauftrag), die nicht nur einen Informationsfluß, sondern reale Transaktionen zur Folge haben.
Auftrag	Nutzdatensegment des Kunden an das Kreditinstitut, mit der ein Transaktions- oder Abholauftrag erteilt wird.
Benutzer	Eine natürliche Person, die als Inhaber oder Berechtigter eines Kontos über ein Kundenprodukt/-endgerät Homebanking betreibt (vgl. Kunde).
Datenelement	(DE) Funktionale Untereinheit eines →Segments (z.B. Bankleitzahl). Ausprägungen: Einfache DE, DEG oder GD.
Datenelementgruppe	(DEG) Zu einer logischen und syntaktischen Einheit zusammengefaßte →Gruppenelemente (z.B. Segmentkopf). (Gegensatz: einfaches DE)
Datenstruktur	Oberbegriff für →Nachricht, →Segment, DE, DEG, GD (strukturierte Dateneinheit beliebiger "Ebene").
einfaches DE	Ein →Datenelement, das einen einzigen Wert enthält.
elektronische Signatur	Kryptographisches Authentifikationsmerkmal, das auch zum Schutz gegen Veränderungen der Nachrichten, z.B. bei der Datenübertragung, dient. Hier im einzelnen: Elektronische Unterschrift gemäß DFÜ-Abkommen oder MAC-Verfahren wie in der ZKA-Chipkarte eingesetzt.
Gruppenelement	(GD) Ein →einfaches Datenelement, das ein untergeordneter Teil einer →Datenelementgruppe ist und im →Segment durch seine Position innerhalb der DEG identifiziert wird.
Ini-Brief	Begleitbrief; handschriftlich unterschriebener öffentlicher Schlüssel, der zu dessen Initialisierung an das Kreditinstitut gesandt wird.
Kopfteil	In einheitlichem Format vorangestellter "Header" (Nachrichtenkopf, →Segmentkopf)
Kreditinstitut	Allgemeingültig für die Kreditinstitutseite in Abgrenzung zur Kundenseite.
Kreditinstitutsnachricht	→Nachricht vom Kreditinstitut an den Kunden, die das Ergebnis der →Aufträge des Kunden enthält.
Kunde	1. Allgemeingültig für die Kundenseite in Abgrenzung zum →Kreditinstitut 2. Rolle, in der ein →Benutzer im Rahmen eines Dialoges auftritt
Kundennachricht	→Auftragssatz
Nachricht	Send- bzw. Empfangseinheit, die sich aus →Segmenten zusammensetzt. Es sind →Kundennachrichten und →Kreditinstitutsnachrichten zu unterscheiden.
Nutzdaten	Eigentliche bankfachliche Auftragsdaten (z.B. Überweisung) in Abgrenzung zu technischen Zusatzinformationen (Kopf- und Abschlussteile).

Kapitel:	0	Version:	2.0.1	Homebanking-Computer-Interface (HBCI)
Seite:	6	Stand:	02.02.1998	Kapitel: Inhaltsverzeichnis

Begriff	Bedeutung
öffentlicher Schlüssel	RSA-Public-Key
PC-Banking	Homebanking per Online-DFÜ-Dialog mit dem Kreditinstitut vom PC aus (In Abgrenzung zu T-Online-Homebanking, daß auch an reinen T-Online-Terminals ohne Eigenintelligenz für z.B. die Bildung der elektronischen Signatur betrieben werden kann).
privater Schlüssel	RSA-Private-Key
Rumpfteil	Der gesamte auf den Kopfteil folgende Abschnitt der →Nachricht ("Message-Body").
Segment	(SEG) Funktionale Untereinheit einer →Nachricht (z.B. Auftrag oder Nachrichtenkopf).
Segmentfolge	(SF) Bei der Beschreibung einer Nachricht (ohne syntaktische Bedeutung) zu einer logischen Einheit zusammengefaßte →Segmente (z.B. um die Wiederholbarkeit dieser Gruppe von Segmenten einfach beschreiben zu können).
Segmentkategorie	Die →Segmente, die der Kunde an das Kreditinstitut sendet, sind in die Kategorien "Transaktion" (Auftrag für finanzielle Transaktion) und "Information" (Auftrag zum Informationsabruf) eingeteilt.
Segmentkennung	Kennzeichen im →Segmentkopf zur Bestimmung des Segments.
Segmentkopf	→Datenelementgruppe, die ein →Segment einleitet
Signatur	→elektronische Signatur
Syntaxzeichen	Zeichen mit besonderer Bedeutung im Rahmen der Trennzeichensyntax (z.B. "+" als Kennzeichner des Datenelementendes).
Unterschrift	Wenn nicht ausdrücklich anders vermerkt, sind hierunter →elektronische Signaturen (RSA-EU, MAC) zu verstehen.
User	→Benutzer

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: I
Kapitel: Einleitung	Stand: 02.02.1998	Seite: 1

I. EINLEITUNG

Die vorliegenden Homebanking-Spezifikationen (HBCI) schaffen eine automatisiert nutzbare multibankfähige Homebanking-Schnittstelle. Eine übergangsweise parallele Nutzung bisheriger Kreditinstitutszugänge (Screen-Dialog oder ZKA-Standard von 1987) bleibt hiervon unberührt.

Beschrieben wird die Schnittstelle zwischen Kundenprodukt und Kreditinstituts-system. Um die Multibankfähigkeit zu gewährleisten, ist zusätzlich eine Beschreibung der Schnittstelle zwischen Kundenprodukt und Sicherheitsmedium erforderlich. Daher findet sich in den Anlagen (Kap. VIII.8) eine Spezifikation der Schnittstelle zwischen einem HBCI-Kundenprodukt und einer ZKA-Chipkarte. Zur Kommunikation zwischen dem Kundenprodukt und anderen Sicherheitsmedien (z.B. Diskette) finden sich grundlegende Vorgaben in den betreffenden Kapiteln.

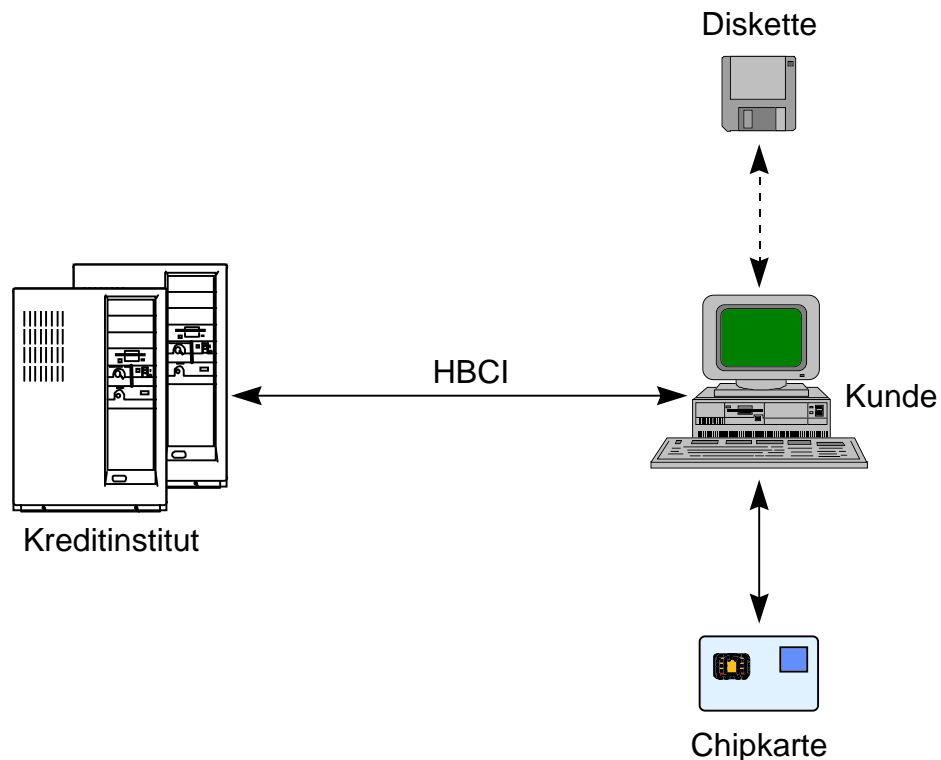



Abb. 1: Übersicht der Schnittstellenbeziehungen

Im Rahmen dieser Schnittstellenbeschreibung findet grundsätzlich keine Spezifikation von Kunden- oder Kreditinstitutssystemen statt. Lediglich werden an einigen gekennzeichneten Stellen Empfehlungen für die Präsentation im Kundenprodukt bzw. für die Verarbeitung im Kreditinstitutssystem gegeben.¹ Diese Ausführungen sind jedoch nicht als Teil der eigentlichen Schnittstellenspezifikation zu verstehen.

Grundsätzlich ist die Schnittstellenbeschreibung plattform- und endgeräteunabhängig. Ein Teil dieser Empfehlungen erfordert jedoch intelligente Endgeräte mit lokaler Speicherintelligenz.

¹ Das Symbol  steht für Hinweise an Kundenprodukthersteller. Das Symbol  bezeichnet Implementierungshinweise für Banksysteme.

Kapitel:	I	Version:	2.0.1	Homebanking-Computer-Interface (HBCI)
Seite:	2	Stand:	02.02.1998	Kapitel: Einleitung

Die HBCI-Spezifikation ist als Schichtenstruktur aufgebaut und somit grundsätzlich unabhängig vom zugrunde liegenden Transportmedium. Um eine einheitliche und multibankfähige Schnittstelle zu gewährleisten, werden jedoch hierzu in den Anlagen (Kap. VIII.6) einige grundsätzliche Festlegungen getroffen.

Die Komprimierung von Nachrichten ist in der derzeit vorliegenden Version nicht vorgesehen, obwohl Datenformate und Erläuterungen bereits dafür vorbereitet sind.

Für einzelne Teile der Schnittstelle (z.B. Signatur, Verschlüsselung und Standard-Finanzdatenformate) wird in den Anlagen auf weitere allgemein zugängliche Spezifikationen verwiesen.

HBCI beschreibt in Kapitel VII eine Vielfalt von Geschäftsvorfällen zwischen Kunde und Kreditinstitut. Da hiermit jedoch nicht sämtliche Anforderungen aller beteiligten Kreditinstitute abgebildet werden können, steht es den ZKA-Verbänden frei, eigene Geschäftsvorfälle, die in diesem Dokument nicht enthalten sind, zu definieren und anzubieten. Die Klassifizierung in ZKA-weit definierte und verbandsspezifische Geschäftsvorfälle erfolgt dabei über die erste Stelle der jeweiligen Segmentkennung (s. Kap. II.6.1).

Es werden folgende Segmentkennungen reserviert:

'Hxxxx': ZKA-weit verabschiedete Geschäftsvorfälle

'Bxxxx': Geschäftsvorfälle für den Bundesverband deutscher Banken e.V.

'Dxxxx': Geschäftsvorfälle für den Deutschen Sparkassen- und Giroverband e.V.

'Gxxxx': Geschäftsvorfälle für den Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V.

'Vxxxx': Geschäftsvorfälle für den Bundesverband Öffentlicher Banken e.V.

'Xxxxx': Bilateral vereinbarte Geschäftsvorfälle anderer Verbände/Institutionen

Die Vergabe und Koordination der mit 'H' und 'X' beginnenden Kennungen übernimmt der ZKA. Die Vergabe und Koordination der übrigen Kennungen übernehmen die jeweiligen Verbände. Kennungen, die diesen Definitionen nicht entsprechen, sind nicht zulässig.

HBCI wird schrittweise um weitere Geschäftsvorfälle ergänzt werden. Für die nächste Version sind z.Zt. unter anderem folgende Geschäftsvorfälle geplant:

- Wertpapierorder
- Abruf von Börsenkursen
- Abruf von Einzelumsätzen
- Auslandsüberweisung ohne Meldeteil
- Laden der elektronischen Geldbörse

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: I
Kapitel: Einleitung	Stand: 02.02.1998	Seite: 3

Für weitere Fragen und Informationen zu HBCI wenden Sie sich bitte an eine der nachfolgenden Adressen:

Organisation	Ansprechpartner	Telefon	Telefax
Bundesverband deutscher Banken e.V., Köln	Herr Fontaine	0221/1663-203	0221/1663-222
Bank-Verlag GmbH	Herr Junghanns	0221/5490-199	0221/5490-130
Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V., Bonn	Herr Steinhaus	0228/509-172	0228/509-201
Deutscher Sparkassen- und Giroverband e.V., Bonn	Herr Ewens	0228/204-353	0228/204-250
 IZ, Informatikzentrum der Sparkassenorganisation GmbH, Bonn	Herr Dünnwald	0228/4495-429	0228/4495-640
Bundesverband Öffentlicher Banken Deutschlands e.V., Bonn	Frau Theisen-Wacket	0228/8192-290	0228/8192-222
HBCI-Leitstelle des ZKA c/o  IZ, Informatikzentrum der Sparkassenorganisation GmbH, Bonn	Herr Stein	0228/4495-670	0228/4495-640

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Zeichensatz	Stand: 02.02.1998	Seite: 5

II. NACHRICHTENAUFBAU

II.1 Zeichensatz.....	7
II.2 Syntax	8
II.3 Nachrichtenelemente	9
II.3.1 Datenelemente	9
II.3.2 Datenelementgruppen.....	9
II.3.3 Segmente	9
II.3.4 Segmentfolgen	9
II.3.5 Nachrichten	9
II.4 Festlegungen	11
II.4.1 Entwertung	11
II.4.2 Binäre Daten	11
II.4.3 Transparente Daten	11
II.4.4 Stati	11
II.4.5 Datenstruktur-Längenangaben.....	12
II.4.6 Datum und Uhrzeit	12
II.4.7 Auslassen von Datenstrukturen.....	13
II.5 Datenformate	15
II.5.1 Basisformate	15
II.5.2 Abgeleitete Formate	16
II.5.3 Mehrfach verwendete Elemente.....	17
II.5.3.1 Betrag	17
II.5.3.2 Kreditinstitutskennung.....	18
II.5.3.3 Kontoverbindung.....	19
II.5.3.4 Saldo.....	19
II.5.3.5 Adresse.....	20
II.6 Steuerstrukturen	21
II.6.1 Segmentkopf	21
II.6.2 Nachrichtenkopf	23
II.6.3 Nachrichtenabschluß.....	25
II.7 Kundennachrichten allgemein.....	26
II.7.1 Allgemeiner Nachrichtenaufbau	26
II.7.2 Aufträge.....	28
II.7.3 Abholauftrag.....	29

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 6	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Zeichensatz

II.8 Kreditinstitutsnachrichten allgemein	33
II.8.1 Allgemeiner Nachrichtenaufbau	33
II.8.2 Rückmeldungen zur Gesamtnachricht.....	34
II.8.3 Rückmeldungen zu Segmenten	35
II.8.4 Datensegmente	36
II.8.5 RückmeldungsCodes	37
II.8.5.1 Grundkonzept	37
II.8.5.2 Rückmeldung	37
II.8.5.3 Reaktionsvorschriften	40
II.8.5.4 Code-Bedeutungen.....	42
II.8.5.4.1 Erfolgsmeldungen	42
II.8.5.4.2 Warnungen und Hinweise.....	42
II.8.5.4.3 Fehlermeldungen	43
II.9 Allgemeiner Nachrichtenaufbau bei Verschlüsselung.....	46

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Zeichensatz	Stand: 02.02.1998	Seite: 7

II.1 Zeichensatz

Der HBCI-Basiszeichensatz baut auf dem international normierten Zeichensatz ISO 8859 auf. Im DE „Unterstützte Sprachen“ in die Bankparameterdaten (s. Kap. IV.2) stellt das Kreditinstitut den jeweiligen Codeset des ISO 8859 ein.¹ Ferner wird in die BPD der sprachenspezifische Subset des ISO 8859 eingestellt. Codeset und Subset definieren gemeinsam den HBCI-Basiszeichensatz. Dieser gilt grundsätzlich für sämtliche nicht-binären Datenelemente. Sofern hiervon aufgrund von Verarbeitungsrestriktionen abgewichen wird, ist dies bei der jeweiligen Formatbeschreibung vermerkt. Für transparente Daten gilt der jeweilige Zeichensatz des Fremdformats.

Kreditinstitutsseitig ist jeweils der vollständige erlaubte Zeichensatz zu unterstützen. HBCI-Syntaxzeichen (s.o.) bleiben von den Zeichensatzvorgaben unberührt (d.h. sind stets erforderlich und mit fester Codierung vorgegeben).

Wird ein Auftrag an ein Kreditinstitut übermittelt, der hinsichtlich Zeichensatz und Codierung nicht den Richtlinien entspricht, so ist dieser abzuweisen. Eine kreditinstitutsseitige Korrektur der Auftragsdaten erfolgt nicht.

¹ Z.Zt. ist lediglich Codeset 1 (Latin 1) zugelassen.

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 8	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Syntax

II.2 Syntax

Es wird eine Trennzeichensyntax mit Freigabezeichen verwendet, die sich, neben vielen anderen Anwendungen, auch in EDIFACT bewährt hat.

Folgende Syntaxzeichen werden vereinbart:

Zeichen	Bedeutung
+	Datenelement (DE)-Trennzeichen
:	Gruppendatenelement (GD)-Trennzeichen
'	Segmentende-Zeichen
?	Freigabezeichen
@	Binärdatenkennzeichen

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Nachrichtenelemente	Stand: 02.02.1998	Seite: 9

II.3 Nachrichtenelemente

II.3.1 Datenelemente

Datenelemente (DE) sind die kleinsten syntaktischen Informationseinheiten. Datenelemente werden durch das DE-Trennzeichen '+' syntaktisch getrennt.

...+DE+DE+DE+...

II.3.2 Datenelementgruppen

Zusammengehörende Daten können zu einer syntaktischen Einheit zusammengefaßt werden. Diese Datenelementgruppen (DEG) bestehen wiederum aus Gruppenelementen (GD). Gruppenelemente werden durch das GD-Trennzeichen ':' getrennt. Die Datenelementgruppe wird vom vorausgehenden und nachfolgenden Element wie ein DE durch das DE-Trennzeichen getrennt. Jede DEG kann beliebig viele GD enthalten. Datenelementgruppen können nicht Bestandteil einer Datenelementgruppe sein.

...+DE+GD:GD:GD:GD+DE+...

II.3.3 Segmente

Datenelemente und Datenelementgruppen setzen sich zu Segmenten zusammen. Jedes Segment enthält bestimmte zusammengehörige Informationen (z.B. Steuerinformationen, Nutzdaten oder Signatur). Die Segmente werden ausschließlich in der angegebenen Reihenfolge eingestellt, sofern eine Reihenfolge vorgegeben ist.

Jedes Segment wird mit der DEG „Segmentkopf“ (s.u.) eingeleitet. Das Ende eines Segmentes wird stets durch das Segmentende-Zeichen (') signalisiert. Vor dem ersten und nach dem letzten DE eines Segments darf kein DE-Trennzeichen erscheinen.

Allgemeiner Segmentaufbau:

Segmentkopf+DE+DE+...+DE'

II.3.4 Segmentfolgen

Eine Segmentfolge beschreibt eine Gruppe von Segmenten, die nur gemeinsam auftreten dürfen. Dabei handelt es sich nicht um eine syntaktische, sondern nur um eine logische Definition.

II.3.5 Nachrichten

Die Kommunikation zwischen Kunde und Kreditinstitut erfolgt bei HBCI über Nachrichten. Nachrichten setzen sich aus einer vorgegebenen Segmentabfolge zusammen (s. Abb. 2). Ausnahmslos alle Nachrichten (Kunde an Kreditinstitut und umgekehrt) enthalten je ein Kopf- und ein Abschlußsegment. Alle weiteren Nachrichteninhalte werden ebenfalls in Segmente, die vom Aufbau her dem allgemeinen festen Segmentformat entsprechen, eingestellt. Der allgemeine Nachrichtenaufbau (Segmentabfolge) ist in den jeweiligen Kapiteln zu Kunden- und Kreditinstitutsnachrichten beschrieben.

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 10	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Nachrichtenelemente

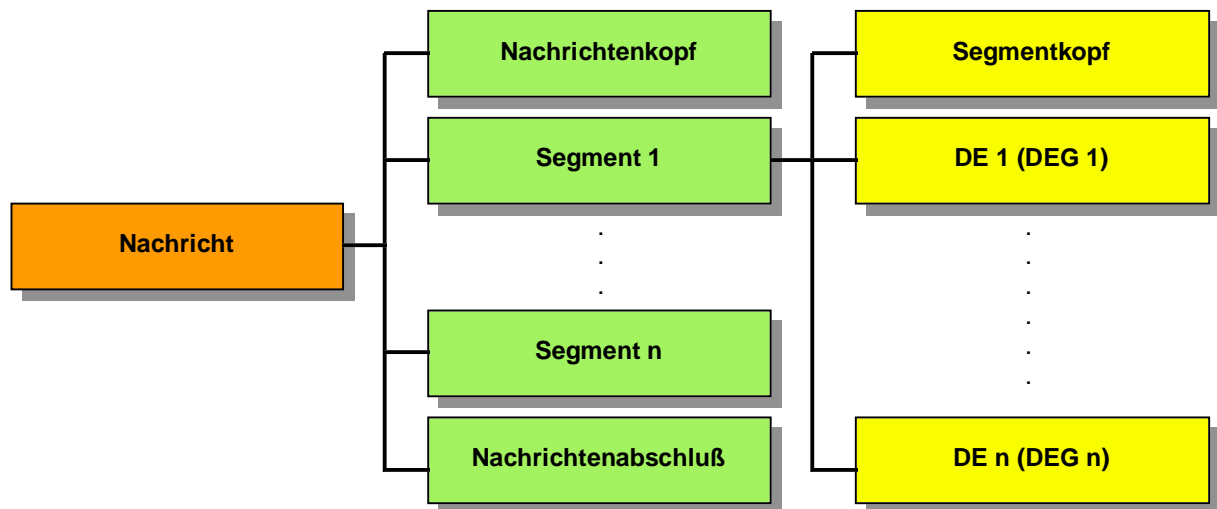


Abb. 2: Nachrichtenaufbau

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Festlegungen	Stand: 02.02.1998	Seite: 11

II.4 Festlegungen

II.4.1 Entwertung

Kommen Syntaxzeichen in einzustellenden Daten vor, sind diese durch Voranstellung des Freigabezeichens '?' zu entwerten. Die Entwertung hat bei allen einzustellenden Daten, außer bei binären Daten zu erfolgen.

Beispiel 1:

vor Entwertung: Taschengeld für Hans + Franz
nach Entwertung: Taschengeld für Hans ?+ Franz

Beispiel 2:

vor Entwertung: Ist das so richtig??
nach Entwertung: Ist das so richtig????

II.4.2 Binäre Daten

Für binäre Daten gilt eine besondere Syntaxregelung: Das Auftreten dieser Daten wird eingeleitet mit dem Binärdatenkennzeichen (@). Anschließend folgt die Längenangabe zu den binären Daten und der binäre Wert selbst, der ebenfalls mit dem Binärdatenkennzeichen eingeleitet wird. Die Länge wird angegeben in Byte (nicht die Länge der darstellbaren Zeichen). Hierzu muß sichergestellt sein, daß der binäre Datenstrom in vollen Byte dargestellt werden kann (*binäre Daten, die nicht im Byteformat vorliegen, können nicht über HBCI transportiert werden*). Syntaxzeichen, die in binären Daten auftreten, dürfen nicht als solche interpretiert werden.

...+DE+@<Länge>@<Binärdaten>+DE...

II.4.3 Transparente Daten

Im Rahmen dieser Schnittstelle werden gegebenenfalls Daten gemäß anderer Standards und Formate (z.B. DTAUS, MT 940) transparent eingestellt. Diese transparent eingestellten Daten werden wie binäre Daten behandelt. Somit haben die Belegungs- und Formatregeln (auch Zeichensatzkonventionen) des HBCI-Standards an dieser Stelle keinen Einfluß. An dessen Stelle treten die Belegungs- und Formatregeln des jeweiligen Formatstandards. Institutsindividuelle Belegungen sind bei transparenten Formaten nicht zugelassen.

II.4.4 Stati

Alle Datenstrukturen sind durch einen Existenzstatus beschrieben. Folgende Stati sind möglich:

Code	Bedeutung	Erläuterung
M	Muß	Datenstruktur muß vorhanden sein und ist inhaltlich korrekt zu füllen
K	Kann	Datenstruktur ist optional

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 12	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Festlegungen

Bei allen Datenstrukturen ist eine variable Anzahl (Schreibweise: m..n) möglich. Dies bedeutet, daß die Struktur m-mal den Status „Muß“ und (n-m)-mal den Status „Kann“ aufweist.

Die Stati beziehen sich jeweils auf die beschriebene Syntaxebene. Stati übergeordneter Syntaxebenen sind hiervon unbenommen.

Beispiel: Eine DEG hat den Status 'Kann', ihre GDs haben den Status 'Muß'.

Bedeutung: Die DEG kann optional eingestellt werden. Wenn sie jedoch eingestellt wird, müssen alle GD, die den Status 'Muß' haben, gefüllt werden.

Bei numerischen „Kann“-Elementen ist zwischen der Nichtbelegung und der Belegung mit dem Wert 0 zu unterscheiden.

Beispiel: Stellt das Kreditinstitut in das Kann-DE „Dispokredit“ den Wert '0' ein, bedeutet dies, daß dem Kunde kein Kredit zur Verfügung steht. Stellt es dagegen das DE nicht ein, so ist keine Interpretation des Kreditrahmens möglich.

Wenn DE bzw. GD mit dem Status „Kann“ mehrfach auftreten können (Anzahl > 1), dürfen sie nur als letztes Element der jeweiligen syntaktischen Einheit eingestellt werden.

II.4.5 Datenstruktur-Längenangaben

Die Zahlen in der Tabellenspalte "Länge" geben jeweils die Datenstruktur-Länge in Byte an. Es ist zwischen Maximal- und Festlängen zu unterscheiden. Sind der Längenangabe 2 Punkte '..' vorangestellt, so handelt es sich um eine Maximallänge. In diesem Fall darf die eingestellte Datenstruktur auch eine geringere Länge aufweisen. Bei Festlängen dagegen führt jede Abweichung von der angegebenen Längenangabe zu einem Syntaxfehler.

Die Angabe '..' ohne Ziffern kennzeichnet ein DE bzw. GD beliebiger Länge (z.B. externe Datenformate). Bei abgeleiteten Datenformaten (z.B. Datum, Uhrzeit) ist die maximale Länge durch die Formatdefinition vorgegeben. Dieser Fall ist durch ein '#' im Längenfeld gekennzeichnet. DEG besitzen weder ein Längen- noch ein Formatfeld, da sich die Länge einer DEG aus der Summe der Längen der zugehörigen GD ergibt. Die Länge von Binärdaten wird im Segment durch ein vorangestelltes Längenfeld angegeben.

II.4.6 Datum und Uhrzeit

Generell besitzen Datums- und Uhrzeitangaben, die von Kundensystemen automatisch generiert werden (z.B. Zeitpunkt der Signatur), keinen rechtsverbindlichen Charakter, da nicht davon ausgegangen werden kann, daß Kundensysteme diese Daten korrekt erzeugen.

Datum und Uhrzeit, die vom Kundensystem gesendet werden, besitzen somit keine verarbeitungstechnische Bedeutung, sondern lediglich dokumentarischen Charakter. Dies bezieht sich nicht auf Datums- und Uhrzeitangaben, die vom Kunden selbst eingegeben werden (z.B. Ausführungsdatum von terminierten Überweisungen).

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Festlegungen	Stand: 02.02.1998	Seite: 13

II.4.7 Auslassen von Datenstrukturen

♦ Auslassen von Segmenten

Kann-Segmente, die keine Daten enthalten, werden einschließlich ihres Segmentkopfes ausgelassen.

♦ Auslassen von Datenelementen

DE werden anhand ihrer Reihenfolge innerhalb des Segmentes identifiziert. DE für die kein Inhalt vorhanden ist, können, sofern sie den Status „Kann“ haben, ausgelassen werden. Ihre Position wird, sofern noch signifikante (mit Inhalt gefüllte) DE folgen, durch ein DE-Trennzeichen dargestellt.

Beispiel 1:

```
Segmentkopf+DE+DE+++DE+DE+DE '
```

Die DE 3 und 4 nach dem Segmentkopf wurden ausgelassen.

♦ Auslassen von Datenelementen durch Abschneiden

Ist für DE, die am Ende eines Segments stehen, kein Inhalt vorhanden, können sie ausgelassen werden. In diesem Fall wird das Segmentende-Zeichen unmittelbar nach dem letzten mit Inhalt belegten DE angegeben.

Beispiel 2:

```
Segmentkopf+DE+DE+++DE '
```

In Fortführung von Beispiel 1 wurden die letzten beiden DE (6. und 7. DE nach dem Segmentkopf) abgeschnitten.

♦ Auslassen von Gruppendatenelementen

Es gelten analog die Ausführungen zur Auslassung von Datenelementen.

Beispiel 3:

```
Segmentkopf+DE+GD:GD+GD:::GD '
```

In der letzten Datenelementgruppe wurden zwei GD ausgelassen.

♦ Auslassen von Gruppendatenelementen durch Abschneiden

Falls ein oder mehrere GD am Ende einer DEG ausgelassen werden, können sie durch das DE-Trennzeichen abgeschnitten werden. Stehen sie als letzte im Segment, wird das Segmentende-Zeichen unmittelbar nach dem letzten mit Inhalt belegten GD angegeben.

Beispiel 4:

```
Segmentkopf+DE+GD+GD '
```

In Fortführung von Beispiel 3 wurde das letzte GD im zweiten DE (erste DEG) nach dem Segmentkopf unterdrückt. Die letzten drei GD in der letzten DEG wurden abgeschnitten.

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 14	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Festlegungen

Kann-DE sollten am Ende des Segmentes stehen, um eine Reduzierung des Datenvolumens durch Abschneiden zu ermöglichen, sofern dies keine Auswirkungen auf die logische Reihenfolge der Daten hat. Ebenso sollten Kann-GD am Ende einer DEG stehen.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Datenformate	Stand: 02.02.1998	Seite: 15

II.5 Datenformate

II.5.1 Basisformate

Grundsätzlich sind Daten nicht durch Leerzeichen auf feste Längen aufzufüllen. Alphanumerische Daten und hieraus abgeleitete Formate müssen, bevor sie in die HBCI-Nachricht eingestellt werden, um führende und nachfolgende Leerzeichen gekürzt werden, sofern die Leerzeichen nicht inhaltlich signifikant sind.²

Name	Ken-nung	Beschreibung
Alphanumerisch	an	Sofern nicht anders vermerkt, gilt der HBCI-Basiszeichensatz. Die Zeichen CR und LF sind ausgeschlossen.
Text	txt	Es gilt der vollständige HBCI-Basiszeichensatz.
Numerisch	num	Zulässig sind lediglich die Ziffern '0' bis '9'. Führende Nullen sind nicht zugelassen.
Ziffern	dig	Zulässig sind die Ziffern '0' bis '9'. Führende Nullen sind zugelassen.
Fließkommadarstellung	float	Es gelten die Ausführungen zu numerischen Daten. Zusätzlich ist als Dezimaltrennzeichen das Komma erlaubt. Es gilt die S.W.I.F.T.-Notation, d.h. Nachkommastellen mit dem Wert 0 sind von rechts zu kürzen. Als Dezimaltrennzeichen dient das Kommazeichen ','. Dieses darf nicht entfallen. Beispiele: 100,00 → 100, 100,20 → 100,2 4.567,89 → 4567,89
Binär	bin	Binäre Daten werden unverändert in den HBCI-Datensatz eingestellt. Eine Umwandlung in eine Zeichendarstellung erfolgt nicht. Es ist zu beachten, daß der HBCI-Basiszeichensatz für binäre Daten keine Gültigkeit besitzt. Ferner gelten die speziellen Syntaxregeln für binäre Daten (s. Kap. II.4.2).

² Falls führende oder nachfolgende Leerzeichen eine inhaltliche Bedeutung haben können (z.B. Verwendungszweckzeilen), so ist dies in der Beschreibung des jeweiligen Datenelementes angegeben.

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 16	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Datenformate

II.5.2 Abgeleitete Formate

Nachstehende aus den oben genannten Basisformaten abgeleitete Formate haben stets den folgenden Aufbau:

Name	Ken- nung	Basis- format	Län- ge	Beschreibung
Ja/Nein	jn	an	1	Format: J bzw. N (in Großbuchstaben) Hat das DE den Status „Kann“, so gilt bei Auslassung der Standardwert „N“.
Datum	dat	num	8	Format: JJJJMMTT Erlaubt sind alle existenten Datumsangaben.
Virtuelles Datum	vdat	num	8	Format: JJJJMMTT Erlaubt sind auch die nicht existenten Datumsangaben 29.02. und 30.02 z.B. als Valutadatum für Zinsabschlüsse.
Uhrzeit	tim	dig	6	Format: hhmmss Gültige Uhrzeit. Es ist immer Ortszeit des sendenden System einzustellen. Unterschiedliche Zeitzone werden nicht unterstützt
Identifikation	id	an	..30	dient der eindeutigen Kennzeichnung von Objekten (z.B. Benutzerkennung, Kontonummer)
Länderkennzeichen	ctr	dig	3	Kennzeichen gemäß ISO 3166-1 (numerischer Code) ³
Währung	cur	an	3	Kennzeichen gemäß ISO 4217 (alphabetischer Code) in Großbuchstaben ⁴
Wert	wrt	float	..15	Fließkommabetrags (z.B. für Wertbeträge oder Zinssätze)

³ s. Kap. VIII.11

⁴ s. Kap. VIII.11

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Datenformate	Stand: 02.02.1998	Seite: 17

II.5.3 Mehrfach verwendete Elemente

Um wiederholt auftretende Strukturen von Datenelementen definieren zu können, werden diese zu 'mehrfach verwendeten Elementen' (MVE) zusammengefaßt.

Name	Kennung
Betrag	btg
Kreditinstitutskennung	kik
Kontoverbindung	kto
Saldo	sdo
Adresse	adr

Es ist zu beachten, daß es sich bei den mehrfach verwendeten Elementen nicht um syntaktische Elemente (z.B. Datenelementgruppen) handelt. Vielmehr treten diese lediglich in identischer Reihenfolge und Formatierung stets gemeinsam auf. Mehrfach verwendete Elemente können als Datenelementgruppe (DEG) oder Gruppenelement-Gruppe (GDG), nicht jedoch als Datenelement eingestellt werden. Über die jeweilige Ausprägung entscheidet die Definition auf Geschäftsvorfallebene. Treten mehrfach verwendete Elemente auf derselben syntaktischen Ebene wie benachbarte Elemente auf, so dürfen sie nicht durch Auslassen von Kann-Elementen (s. Kap. II.4.7) gekürzt werden (s. Bsp. 2 und 4).

Beispiel 1: Saldo als DEG

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Kontobezeichnung	DE	an	..35	M	1	
2	Kontosaldo	DEG	sdo	#	M	1	
3	Beschreibung	DE	an	..35	M	1	

Girokonto+C:1000, :DEM:19960701+Beschreibung

Beispiel 2: Saldo als GDG

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Kontobezeichnung	GD	an	..35	M	1	
2	Kontosaldo	GDG	sdo	#	M	1	
3	Beschreibung	GD	an	..35	M	1	

Girokonto:C:1000, :DEM:19960701::Beschreibung

II.5.3.1 Betrag

◆ Format

Name: Betrag
Typ: Mehrfach verwendetes Element
Kennung: btg

Nr.	Name	Typ	For-	Län-	Sta-	An-	Restriktionen
-----	------	-----	------	------	------	-----	---------------

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 18	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Datenformate

			mat	ge	tus	zahl	
1	Wert	#	wrt	#	M	1	
2	Währung	#	cur	#	M	1	

◆ Erläuterungen

In Vorbereitung auf die EWWU wird jeder Wertbetrag zusammen mit einem Währungskennzeichen gemäß ISO 4217 (alphabetischer Code) übertragen.

Es ist maximal die gemäß ISO 4217 gültige Anzahl Nachkommastellen der jeweiligen Währung (z.B. 2 bei DM) einzustellen. Eine höhere Anzahl führt zu einer entsprechenden Fehlermeldung und zur Ablehnung des Auftrags. Die maximale Stellenzahl kann eventuell nicht in allen Währungen verarbeitet werden, obwohl der Betrag syntaktisch korrekt definiert wurde. In diesem Fall wird der Auftrag mit einer entsprechenden Meldung abgelehnt.

◆ Beispiel

4567,89 : DEM

II.5.3.2 Kreditinstitutskennung

◆ Format

Name: Kreditinstitutskennung
Typ: Mehrfach verwendetes Element
Kennung: kik

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Länderkennzeichen	#	ctr	#	M	1	
2	Kreditinstitutscode	#	an	..30	K	1	

◆ Erläuterungen

Nr. 1: Länderkennzeichen

Es ist das numerische Länderkennzeichen des Instituts gemäß ISO 3166 (numerischer Code) anzugeben.

Nr. 2: Kreditinstitutscode

Es ist eine landesspezifische Kennung anzugeben, die das Kreditinstitut eindeutig identifiziert. In Deutschland wird die Bankleitzahl eingestellt. Bei Kreditinstituten, die in Ländern ohne Institutskennungssystem beheimatet sind, kann die Belegung entfallen.

◆ Beispiel

280 : 10020030

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Datenformate	Stand: 02.02.1998	Seite: 19

II.5.3.3 Kontoverbindung

◆ Beschreibung

Anhand dieses Formats können sowohl deutsche als auch internationale Bankverbindungen beschrieben werden.

◆ Format

Name: Kontoverbindung
Typ: Mehrfach verwendetes Element
Kennung: kto

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Konto-/Depotnummer	#	id	#	M	1	
2	Kreditinstitutskennung	#	kik	#	M	1	

◆ Erläuterungen

Nr. 1: Konto-/Depotnummer

Es ist die jeweilige Identifikationsnummer des Kontos einzustellen (Kontonummer, Depotnummer, Kreditkartennummer etc.). Das DE dient auch zur Aufnahme von internationalen (alphanumerischen) Kontonummern und zukünftig 20-stelligen Kreditkartenkontonummern.

Nr. 2: Kreditinstitutskennung

s. II.5.3.2

◆ Beispiel

1234567:280:10020030



Den Herstellern von Kundensystemen wird empfohlen, eine Bankleitzahlendatenbank zu hinterlegen, um eine Plausibilitätsprüfung von Bankleitzahlen und eventuell auch Kontonummern zu ermöglichen und den Kunden ggf. Bankleitzahlen über Auswahl des Kreditinstitutnamens ermitteln zu lassen.

II.5.3.4 Saldo

◆ Format

Name: Saldo
Typ: Mehrfach verwendetes Element
Kennung: sdo

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 20	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Datenformate

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Soll-Haben-Kennzeichen	#	an	1	M	1	C, D
2	Wert	#	wrt	#	M	1	
3	Währung	#	cur	#	M	1	
4	Datum	#	dat	#	M	1	
5	Uhrzeit	#	tim	#	K	1	

♦ Erläuterungen

Nr. 1: Soll-Haben-Kennzeichen

Code	Bedeutung
C	Credit (Haben)
D	Debit (Soll)

Nr. 4: Datum

Es ist das Datum der Übertragung des Saldos einzustellen.

Nr. 5: Uhrzeit

Es ist die Uhrzeit der Übertragung des Saldos einzustellen.

♦ Beispiel

C:1000, :DEM:19960710:123015

II.5.3.5 Adresse

♦ Format

Name: Adresse
Typ: Mehrfach verwendetes Element
Kennung: adr

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Name 1	#	an	..35	M	1	
2	Name 2	#	an	..35	K	1	
3	Straße/Postfach	#	an	..35	M	1	
4	PLZ/Ort	#	an	..35	M	1	
5	Telefon	#	an	..35	K	1	

♦ Beispiel

Ernst Müller::Bahnhofstr. 17:12345 Berlin

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Steuerstrukturen	Stand: 02.02.1998	Seite: 21

II.6 Steuerstrukturen

II.6.1 Segmentkopf

◆ Beschreibung

Jedes Segment beginnt mit nachstehender DEG. Im Unterschied zu Nachrichten enthalten Segmente jedoch keinen Abschlußteil, da das Segmentende durch das Segmentende-Zeichen markiert ist.

◆ Format

Name: Segmentkopf
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkennung	GD	an	..6	M	1	
2	Segmentnummer	GD	num	..3	M	1	>=1
3	Segmentversion	GD	num	..3	M	1	
4	Bezugssegment	GD	num	..3	K	1	>=1

◆ Erläuterungen

Nr. 1: Segmentkennung

Es ist die segmentspezifische Kennung einzustellen, die jedem Segment bzw. Auftrag zugeordnet ist (z.B. "HKUEB" für "Einzelüberweisung"). Die Angabe hat in Großschreibung zu erfolgen.

Nr. 2: Segmentnummer

Die Segmentnummer dient der eindeutigen Identifizierung eines Segments innerhalb einer Nachricht. Die Segmente einer Nachricht werden in Einzelschritten streng monoton aufsteigend numeriert. Die Numerierung beginnt mit 1 im ersten Segment der Nachricht (Nachrichtenkopf).

Nr. 3: Segmentversion

Die Segmentversion von administrativen Segmenten⁵ wird bei jeder Änderung des Segmentformats inkrementiert. Bei Geschäftsvorfallssegmenten wird die Segmentversion auf logischer Ebene verwaltet, d.h. sie ist für das Auftrags-, das Antwort- und das Parametersegment des Geschäftsvorfalles stets identisch und wird inkrementiert, wenn sich das Format von mindestens einem der drei Segmente ändert.

Dieses Verfahren gilt bei Standardsegmenten einheitlich für alle Kreditinstitute. Bei verbandsindividuellen Segmenten obliegt die Versionssteuerung dem jeweiligen Verband. Der Zeitpunkt der Unterstützung einer neuen Segmentversion kann jedoch zwischen den Verbänden variieren.

⁵ Die Segmentart 'Administration' bzw. 'Geschäftsvorfall' ist bei jeder Segmentbeschreibung angegeben.

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 22	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Steuerstrukturen

Die für die jeweilige HBCI-Version gültige Segmentversion ist bei der jeweiligen Segmentbeschreibung vermerkt.



Falls der Kunde ein Segment mit einer veralteten Versionsnummer einreicht, sollte ihm in einer entsprechenden Warnung rückgemeldet werden, daß sein Kundenprodukt aktualisiert werden sollte.

Nr. 4: Bezugssegment

Sofern sich ein Kreditinstitutssegment auf ein bestimmtes Kundensegment bezieht (z.B. Antwortrückmeldung auf einen Kundenauftrag) hat das Kreditinstitut die Segmentnummer des Segments der Kundennachricht einzustellen, auf das sich das aktuelle Segment bezieht (s. DE „Segmentnummer“). In Zusammenhang mit den Angaben zur Bezugsnachricht aus dem Nachrichtenkopf ist hierdurch eine eindeutige Referenz auf das Segment einer Kundennachricht möglich.

Falls die Angabe eines Bezugssegments erforderlich ist, ist dieses bei der Formatbeschreibung eines Kreditinstitutssegments angegeben.

Dieses DE darf nur in Kreditinstitutssegmente eingestellt werden.

♦ Beispiel

HIKAZ:5:1:3

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Steuerstrukturen	Stand: 02.02.1998	Seite: 23

II.6.2 Nachrichtenkopf

◆ Beschreibung

Nachstehender Kopfteil führt alle Kunden- und Kreditinstitutsnachrichten an.

◆ Format

Name: Nachrichtenkopf
 Typ: Segment
 Segmentart: Administration
 Kennung: HNHBK
 Bezugssegment: -
 Segmentversion: 2
 Sender: Kunde/Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Nachrichtengröße	DE	dig	12	M	1	
3	HBCI-Version	DE	num	..3	M	1	201
4	Dialog-ID	DE	id	#	M	1	
5	Nachrichtennummer	DE	num	..4	M	1	>0
6	Bezugsnachricht	DEG			K	1	

◆ Erläuterungen

Nr. 2: Nachrichtengröße

Es ist die Größe der Nachricht (nach Verschlüsselung und Komprimierung) in Byte einzustellen. Das DE ist mit führenden Nullen auf die vorgegebene feste Länge aufzufüllen. Dies ist erforderlich, damit die Nachrichtenlänge nicht mit der Länge des DE variiert.

Nr. 3: HBCI-Version

Die HBCI-Version [entspricht der](#) Version der Schnittstellenspezifikation, [die der jeweiligen Realisierung zugrunde liegt](#) (Bsp.: HBCI-Dokument Version 2.0.1 entspricht '201').

Ein geregelter Dialog ist nur zwischen Systemen möglich, die mit derselben HBCI-Version arbeiten. Stimmt die vom Kunden übermittelte HBCI-Version nicht mit einer der vom Kreditinstitut in den BPD mitgeteilten unterstützten HBCI-Versionen überein, so muß der Dialog vom Kreditinstitut beendet werden. Innerhalb eines Dialoges dürfen nicht Nachrichten unterschiedlicher HBCI-Versionen gesendet werden.

Segment- und HBCI-Versionen werden unabhängig voneinander geführt. Innerhalb eines HBCI-Dialoges dürfen nur [Versionen](#) administrativer Segmente gesendet werden, die der angegebenen HBCI-Version entsprechen. Im Rahmen einer HBCI-Version wird eine Liste der zugehörigen Segmentversionen veröffentlicht ([s. Kap. VIII.1](#)). Weiterhin werden in dieser Liste auch die zusätzlich noch unterstützten Segmentversionen genannt.

Es ist sichergestellt, daß im Segmentkopf die Segmentkennung und Segmentversion unabhängig von der HBCI-Version immer an derselben Stelle

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 24	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Steuerstrukturen

stehen, damit ein Segment auch in späteren HBCI-Versionen immer eindeutig als solches identifiziert werden kann.

Der Zeitpunkt der Unterstützung einer neuen HBCI-Version kann zwischen den [Kreditinstituten](#) variieren.

Die derzeitige HBCI-Version lautet 201. [HBCI-Versionen, die vor dieser Version veröffentlicht wurden, werden kreditinstitutsseitig nicht unterstützt.](#)

Nr. 4: Dialog-ID

Die Dialog-ID dient der eindeutigen Zuordnung einer Nachricht zu einem HBCI-Dialog. Die erste Kundennachricht (Dialoginitialisierung) enthält als Dialog-ID den Wert 0. In der ersten Antwortnachricht wird vom Kreditinstitut eine Dialog-ID vorgegeben, die für alle nachfolgenden Nachrichten dieses Dialogs einzustellen ist. Es ist Aufgabe des Kreditinstituts, dafür zu sorgen, daß diese Dialog-ID dialogübergreifend und systemweit eindeutig ist.

Nr. 5: Nachrichtennummer

Die Nachrichtennummer dient der Referenzierung von Nachrichten innerhalb eines Dialoges. In Zusammenhang mit der Dialog-ID und der Kundensystem-ID können Nachrichten über die Nachrichtennummer auch dialogübergreifend eindeutig referenziert werden. Eine Doppeleinreichungskontrolle ist mit Hilfe der Nachrichtennummer nicht möglich.

Mit Hilfe der Nachrichtennummer numerieren sowohl das Kundensystem als auch das Kreditinstitutssystem seine Nachrichten unabhängig voneinander innerhalb eines Dialoges in Einerschritten streng monoton aufsteigend. Die Numerierung beginnt sowohl beim Kunden- als auch beim Kreditinstitutssystem mit der Dialoginitialisierungsnachricht bei '1'. Nachrichten, deren Numerierung nicht streng monoton aufsteigend erfolgt ist, werden institutsseitig bzw. kundenseitig abgelehnt.

Nr. 6: Bezugsnachricht

Diese DEG dient der eindeutigen Referenzierung von Kundennachrichten. Die eindeutige Referenzierung erfolgt anhand der Dialog-ID und der Nachrichtennummer der Kundennachricht. Falls auf eine Dialoginitialisierungsnachricht des Kunden referenziert werden soll, ist nicht die vom Kunden übermittelte Dialog-ID (0), sondern die vom Kreditinstitut neu vergebene Dialog-ID einzustellen.

Es darf nur auf Nachrichten des dialogführenden Benutzers referenziert werden. Eine explizite Angabe der Benutzerkennung als Referenzierungskriterium ist nicht erforderlich, da diese bereits im Signaturkopf spezifiziert wurde.

Diese DEG muß bei allen Kreditinstitutsnachrichten eingestellt werden. Bei Kundennachrichten darf sie dagegen nicht belegt werden.

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Dialog-ID	GD	id	#	M	1	
2	Nachrichtennummer	GD	num	..4	M	1	>0

◆ Beispiel

HNHBK:1:2+000000000319+201+4711+3+4711:3'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Steuerstrukturen	Stand: 02.02.1998	Seite: 25

II.6.3 Nachrichtenabschluß

◆ Beschreibung

Dieses Segment beendet alle Kunden- und Kreditinstitutsnachrichten.

◆ Format

Name: Nachrichtenabschluß
 Typ: Segment
 Segmentart: Administration
 Kennung: HNHBS
 Bezugssegment: -
 Segmentversion: 1
 Sender: Kunde/Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Nachrichtennummer	DE	num	..4	M	1	>0

◆ Erläuterungen

Nr. 2: Nachrichtennummer

Es ist die Nummer der Nachricht einzustellen, die auch im Nachrichtenkopf eingestellt ist.

◆ Beispiel

HNHBS : 5 : 1 + 3 '

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 26	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Kundennachrichten allgemein

II.7 Kundennachrichten allgemein

II.7.1 Allgemeiner Nachrichtenaufbau

◆ Beschreibung

In einer Nachricht sind z.Zt. nur Aufträge einer Geschäftsvorfallsart zugelassen. Dennoch wird redundant in jeden Segmentkopf die Art des Geschäftsvorfalles eingestellt. Dies soll eine im Rahmen zukünftiger Versionen der HBCI-Schnittstellenspezifikation angestrebte Übermittlung von Auftragsnachrichten mit verschiedenartigen Geschäftsvorfällen ermöglichen.

Bezüglich der Reihenfolge der in die Nachricht einzustellenden Aufträge wird keine Vorgabe getroffen. Da die Reihenfolge der Weiterleitung von Aufträgen an die Verarbeitungssysteme institutsspezifisch ist, beeinflusst die Anordnung der Aufträge nicht zwingend die Reihenfolge der Verarbeitung bzw. Ausführung. Insbesondere ist daher auch keine kundenseitige Priorisierung der Aufträge durch deren Anordnung in der Nachricht möglich.



Eine Priorisierung von Aufträgen könnte für den Kunden u.U. wünschenswert sein, wenn bei geringer Deckung des Kontos mehrere Zahlungsaufträge mit unterschiedlicher Priorität ausgeführt werden sollen. In diesem Fall sollten zuerst die wichtigen Aufträge ausgeführt werden. Da die eingereichten Zahlungsaufträge nicht notwendigerweise in dieser Reihenfolge ausgeführt werden, könnte das Kundenprodukt vor dem Versenden automatisch den Kontensaldo (und ggf. Kontokorrentkredit) abfragen und mit der Summe der Zahlungsaufträge vergleichen. Sind alle Aufträge gedeckt, können sie automatisch versendet werden. Bei mangelnder Deckung kann dies dem Kunden mitgeteilt werden, damit er zunächst lediglich die Aufträge mit hoher Priorität einreicht.

Werden in einer Nachricht Aufträge mit verschiedenen Signaturvorschriften gemischt, so werden diejenigen Aufträge der Nachricht ausgeführt, für welche die Signatur ausreichend ist.



Falls der Kunde Aufträge verschiedener Geschäftsvorfälle oder Signaturvorschriften formuliert und diese zusammen abschicken möchte, so obliegt es dem Kundenprodukt, die Aufträge jeweils in Nachrichten mit gleichem Geschäftsvorfall und Signatur aufzuteilen und diese nacheinander zu verschicken.

Das Kundenprodukt sollte grundsätzlich vor dem Senden des Auftrags prüfen, ob der vom Kunden gewählte Geschäftsvorfall für das angegebene Konto zulässig ist. Bspw. können für ein Wertpapierkonto keine Kontoumsätze rückgemeldet werden.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Kundennachrichten allgemein	Stand: 02.02.1998	Seite: 27

◆ Format

Name: Kundennachricht allgemein
Typ: Nachricht
Sender: Kunde

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	M	1..3	s. Kap. VI.5.2
3	Aufträge	SF	#	K	1	s. Kap. II.7.2
4	Signaturabschluß	SEG	HNSHA	M	1..3	s. Kap. VI.5.3
5	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

◆ Erläuterungen

Nr. 2: Signaturkopf

Je nach Nachrichtentyp ist hier die Signatur des Übermittlers bzw. die Signatur des Unterzeichners einzustellen.

Der Signaturkopf darf nur bei Mehrfachsignaturen mehrfach eingestellt werden.

Nr. 3: Aufträge

Die Segmentfolge enthält die Auftragssegmente des Kunden (s. Kap. II.7.2).

Nr. 4: Signaturabschluß

Der Signaturabschluß darf nur bei Mehrfachsignaturen mehrfach eingestellt werden. Die Anzahl der Signaturabschlußsegmente muß mit der Anzahl der Signaturkopfsegmente übereinstimmen.

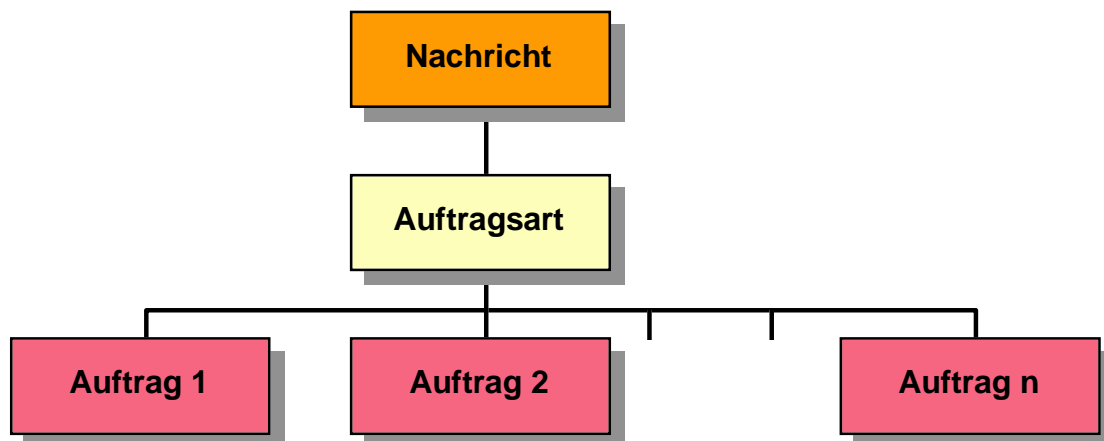


Abb. 3: Logischer Nachrichtenaufbau

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 28	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Kundennachrichten allgemein

II.7.2 Aufträge

◆ Beschreibung

Die Segmentfolge enthält die im Kapitel VII definierten Auftragssegmente des Kunden. Jedes Segment kann dabei beliebig oft und in beliebiger Reihenfolge auftreten. Das Kreditinstitut hat jedoch mit Hilfe der Bankparameterdaten die Möglichkeit, die Art und Anzahl der erlaubten Segmente einzuschränken:

- Die erlaubten Kundensegmente gibt das Kreditinstitut in den Geschäftsvorfallparametern an (s. Kap. IV.6)
- Die maximale Anzahl von Segmenten einer Geschäftsvorfallsarten pro Nachricht kann mit Hilfe des DE „Maximale Anzahl Aufträge“ eingestellt werden (s. Kap. IV.6).
- Die maximale Anzahl von Geschäftsvorfallsarten pro Nachricht kann mit Hilfe des DE „Anzahl Geschäftsvorfallsarten“ eingestellt werden (s. Kap. IV.2).

◆ Format

Name: Aufträge
 Typ: Segmentfolge
 Sender: Kunde

◆ Beispiel

```
HKUEB:3:2+1234567:280:10020030+7654321:280:20030
040+MEIER FRANZ++1000,:DEM+51+000+RE-NR.1234:KD-
NR.9876'
HKKAZ:4:4+1234567:280:10020030++19960701+1996073
0'
HKSAL:5:3+1234567:280:10020030+N'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Kundennachrichten allgemein	Stand: 02.02.1998	Seite: 29

II.7.3 Abholauftrag

◆ Beschreibung

Abholaufträge werden an das Kreditinstitut gesendet, um die institutsseitige Generierung und Übermittlung von spezifischen Informationen einzuleiten (z.B. Kontoumsätze, Börsenkurse). In Abgrenzung dazu haben Transaktionsaufträge nicht nur einen Informationsfluß, sondern reale Transaktionen zur Folge (z.B. Überweisungsauftrag).

Falls im Abholauftrag keine Währung angegeben wird, entspricht die Währung, in der die Kreditinstitutsantwort auf den Abholauftrag erfolgt, stets der Währung des Kundenkontos.

◆ Format

Das Segmentformat ist beim jeweiligen Geschäftsvorfall spezifiziert. Die Erläuterungen beziehen sich auf die dort angegebenen Felder.

◆ Erläuterungen

Kontoverbindung Auftraggeber:

Es ist diejenige Kontoverbindung des Kunden einzustellen, für die im Abholauftrag Daten zurückgemeldet werden sollen. Falls der Abholauftrag nicht in Beziehung zu einem bestimmten Konto steht (z.B. Abruf von Devisenkursen, Abruf des Statusprotokolls), so ist eine beliebige Kontoverbindung des Kunden einzustellen. Es darf nur ein Konto eines Kreditinstituts angegeben werden, für das sich der Kunde im Rahmen der Dialoginitialisierung legitimiert hat.

Von Datum, Bis Datum:

Diese DE dürfen nur gefüllt werden, wenn dies explizit vermerkt ist. Wird kein Zeitraum angegeben, so werden stets alle verfügbaren Einträge zurückgemeldet. Wird ein Zeitraum angegeben, so werden nur diejenigen Einträge zurückgemeldet, die im Zeitraum (einschließlich des Grenzdatums) liegen. Die Eingabemöglichkeiten sind der nachfolgenden Tabelle zu entnehmen. Falls ein Zeitraum angegeben ist, obwohl dieser nicht erlaubt ist, wird der Auftrag abgelehnt. Ebenso wird der Auftrag abgelehnt, wenn der Zeitraum inkonsistent ist (Anfangsdatum größer als Enddatum). Ein Zeitraum darf nicht gleichzeitig mit einem Nummernbereich angegeben werden.

Beispiel:

Von Datum	Bis Datum	Bedeutung
01.07.1996	31.07.1996	liefert alle Einträge, die im angegebenen Zeitraum liegen
01.07.1996	leer	liefert alle Einträge, die am 1.7.96 oder danach angefallen sind
leer	31.07.1996	liefert alle Einträge, die am 31.7.96 oder davor angefallen sind
leer	leer	liefert alle verfügbaren Einträge

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 30	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Kundennachrichten allgemein

Von <Kennung>, Bis <Kennung>:

Hier kann der Abholbereich durch bankfachliche Informationen (z.B. Dauerauftrags-ID, Wertpapiernamen) eingegrenzt bzw. genauer spezifiziert werden, sofern dies durch den betreffenden Geschäftsvorfall unterstützt wird.

Falls die Informationen zu einer bestimmten Kennung (z.B. Kontonummer xy) abgeholt werden sollen, so ist in beide Felder dieselbe Kennung einzutragen.

Im übrigen gelten die Festlegungen zu den Feldern „Von Datum“ und „Bis Datum“.

Aufsetzpunkt:

Falls das Kreditinstitut den Kundenauftrag nicht in einem Auftragssegment beantworten kann, besteht die Möglichkeit, daß es die Beantwortung an einem bestimmten Punkt kontrolliert beendet und dem Kunden in der Antwortnachricht mit dem Rückmeldungscode einen Aufsetzpunkt mitteilt. Dieses kann ein beliebiger institutsinterner Ordnungsbegriff sein, der vom Kundenprodukt nicht interpretiert zu werden braucht. Bei transparenten Daten kann die Fragmentierung beliebig (z.B. logisch oder binär) erfolgen. Es ist lediglich zu fordern, daß die Zusammensetzung der Fragmente im Kundensystem problemlos möglich ist.



Grundsätzlich hat das Kreditinstitutssystem dafür Sorge zu tragen, daß auch bei umfangreichen Abholaufträgen (z.B. Abruf der Kontoumsätze der vergangenen 3 Jahre oder Abruf sämtlicher verfügbarer Börsenkurse) die komplette Information in einem Antwortsegment übertragen wird. D.h. es muß ausgeschlossen sein, daß als Antwort auf einen Abholauftrag dem Kunden wegen zu großer Antwortnachricht nur ein Teil der geforderten Informationen zurückgemeldet wird. Seitens des Kreditinstituts besteht jedoch bei Überschreitung von Zeit- oder Volumengrenzen die Möglichkeit, den Auftrag abzulehnen.



Falls das Kreditinstitut jedoch einen Aufsetzpunkt rückmeldet, wird vom Kundenprodukt erwartet, daß es denselben Abholauftrag unter Hinzufügung des Aufsetzpunktes erneut schickt. In der Antwortnachricht erhält der Kunde den folgenden Teil der Informationen (evtl. inkl. eines erneuten Aufsetzpunktes) rückgemeldet. Dieses Verfahren kann sich solange wiederholen, bis die komplette Informationsmenge übertragen wurde. Die Generierung der Folgenachrichten sollte automatisch, d.h. ohne Einwirkung des Kunden, erfolgen.

Ein Aufsetzpunkt darf vom Kundenprodukt nur dann eingestellt werden, wenn im selben Dialog ein Aufsetzpunkt vom Kreditinstitut rückgemeldet wurde. Nach Beendigung des Dialoges verliert der Aufsetzpunkt seine Gültigkeit.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Kundennachrichten allgemein	Stand: 02.02.1998	Seite: 31

Maximale Anzahl Einträge:

Dieser Parameter dient dazu, die maximale Anzahl rückzumeldender Einträge zu begrenzen. Diese Begrenzung kann auf Wunsch des Kunden erfolgen oder aus technischen Restriktionen des Kundensystems resultieren. So wird Endgeräten, die aufgrund technischer Restriktionen nur eine begrenzte Anzahl rückgemeldeter Einträge (z.B. Umsatzinformationen im Kontoauszug) verarbeiten können, die Möglichkeit gegeben, den Umfang der Institutsnachrichten zu begrenzen. Falls der Kunde keine Begrenzung wünscht, wird das DE ausgelassen. Der Wert 0 ist nicht zulässig.

Falls im angegebenen Bereich weniger Einträge vorliegen als in „Maximale Anzahl Einträge“ angegeben, werden nur die vorliegenden Einträge rückgemeldet. Falls mehr Einträge vorliegen, werden laut untenstehender Tabelle nur <Anzahl> Einträge rückgemeldet. In diesem Fall erhält das Kundensystem im Rückmeldungscode mitgeteilt, daß noch weitere Informationen vorliegen. Im Rückmeldungsparameter wird dem Kundensystem ein Aufsetzpunkt (s.o.) zurückgemeldet, mit Hilfe dessen die über <Anzahl> hinausgehenden Einträge abgerufen werden können.

Beispiel:

Von Datum	Bis Datum	Anzahl	Bedeutung
01.07.1996	31.07.1996	10	liefert die ersten 10 Einträge ab 1.7.96 (sofern mindestens 10 Einträge vorhanden, sonst weniger)
01.07.1996	leer	10	liefert die ersten 10 Einträge ab 1.7.96
leer	31.07.1996	10	liefert die <u>letzten</u> 10 Einträge vor dem 31.07.96
leer	leer	10	liefert von allen verfügbaren Einträgen die <u>letzten</u> 10



Die Einträge werden dem Kunden stets in aufsteigender Reihenfolge rückgemeldet. Eine hiervon abweichende Sortierung (z.B. absteigend oder nach anderen Kriterien) kann das Kundenprodukt bei Bedarf dem Kunden anbieten.

♦ Beispiel

HKKAZ:5:1+1234567+19960701+19960731+10'

♦ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
3010	Es liegen keine Einträge vor
3040	Auftrag nur teilweise ausgeführt
3040	Es liegen weitere Informationen vor
9210	Keine gültige Kontoverbindung des Kunden
9210	Zeitraum hier nicht erlaubt
9210	Kennungen hier nicht erlaubt
9210	Bereichende darf nicht vor Bereichanfang liegen

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 32	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Kundennachrichten allgemein

Code	Beispiel für Rückmeldungstext
9210	Aufsetzpunkt unbekannt

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein	Stand: 02.02.1998	Seite: 33

II.8 Kreditinstitutsnachrichten allgemein

II.8.1 Allgemeiner Nachrichtenaufbau

◆ Beschreibung

Der nachfolgend beschriebene Nachrichtenaufbau bezieht sich auf unverschlüsselte Nachrichten (Aufbau verschlüsselter Nachrichten vgl. Kap. II.9).

◆ Format

Name: Kreditinstitutsnachricht allgemein
Typ: Nachricht
Sender: Kreditinstitut

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	K	1	s. Kap. VI.5.2
3	Rückmeldungen zur Ge- samtnachricht	SEG	HIRMG	M	1	s. Kap. II.8.2
4	Rückmeldungen zu Seg- menten	SEG	HIRMS	K	0..n	s. Kap. II.8.3
5	Datensegmente	SF	#	K	1	s. Kap. II.8.4
6	Signaturabschluß	SEG	HNSHA	K	1	s. Kap. VI.5.3
7	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

◆ Erläuterungen

Nr. 1: Nachrichtenkopf

Allgemeiner Nachrichtenkopf, der auch bei Kundennachrichten verwendet wird.

Nr. 2: Signaturkopf

Falls es das Kreditinstitut wünscht, kann es seine Nachrichten ebenfalls signieren. In diesem Fall hat es dasselbe Signaturverfahren anzuwenden wie der Kunde.

Es ist dem Kreditinstitut freigestellt, ob es als Signatur-ID (vgl. Kap. VI.4 und VI.5.2) die vom Kunden gesendete ID verwendet oder einen eigenen Zähler verwaltet.



Falls Kreditinstitutsnachrichten signiert werden, hat das Kundenprodukt deren Signatur zu prüfen. Falls die Prüfung negativ ausfällt, hat es dem Kunden eine entsprechende Rückmeldung zu geben und den Dialog zu beenden. Falls die Prüfung auch bei einem erneuten Dialog negativ ausfällt, muß von einem Sicherheitsproblem ausgegangen werden.

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 34	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein

II.8.2 Rückmeldungen zur Gesamtnachricht

◆ Beschreibung

In diesem Segment werden Rückmeldungen übermittelt, die sich auf die gesamte Nachricht und nicht auf ein spezifisches Segment beziehen (z.B. „Nachricht entgegengenommen“, „Elektronische Signatur gesperrt“).

◆ Format

Name: Rückmeldungen zur Gesamtnachricht
Typ: Segment
Segmentart: Administration
Kennung: HIRMG
Bezugssegment: -
Segmentversion: 2
Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Rückmeldung	DEG			M	1..99	

◆ Erläuterungen

Nr. 2: Rückmeldung

Format: s. Kap. II.8.5.2

Das DE „Bezugsdatenelement“ ist nicht zu belegen.

Ein Erfolgscode darf nur eingestellt werden, wenn alle Aufträge fehlerfrei sind, d.h. in den Segmenten „Rückmeldungen zu Segmenten“ dürfen in diesem Fall keine Fehlermeldungen gesendet werden.

◆ Beispiel

```
HIRMG:3:2+0010::Nachricht entgegengenommen'
```

```
HIRMG:3:2+9330::Elektronische Signatur gesperrt'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein	Stand: 02.02.1998	Seite: 35

II.8.3 Rückmeldungen zu Segmenten

◆ Beschreibung

Dieses Segment ist genau einmal für jedes Segment der Kundennachricht einzustellen. Hier sind sämtliche RückmeldungsCodes aufzuführen, die sich auf das Kundensegment bzw. die zugehörigen Datenelemente und Datenelementgruppen beziehen. Falls für das jeweilige Kundensegment keine RückmeldungsCodes erzeugt wurden, kann das zugehörige Rückmeldesegment entfallen. Ist das jeweilige Kundensegment fehlerhaft, dann dürfen keine Datensegmente (s.u.) rückgemeldet werden.

◆ Format

Name: Rückmeldungen zu Segmenten
Typ: Segment
Segmentart: Administration
Kennung: HIRMS
Bezugssegment: abhängig von Kundensegment
Segmentversion: 2
Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Rückmeldung	DEG			M	1..99	

◆ Erläuterungen

Nr. 1: Segmentkopf

Als Bezugssegment ist die Segmentnummer des Kundensegments, auf das sich die Rückmeldungen beziehen, einzustellen.

Nr. 2: Rückmeldung

Format: s. Kap. II.8.5.2

Hier sind diejenigen RückmeldungsCodes einzustellen, die sich auf das Segment (Auftrag) bzw. die zugehörigen Datenelemente und Datenelementgruppen beziehen.

◆ Beispiel

```
HIRMS:4:2:5+0010::Auftrag entgegengenommen'
HIRMS:5:2:6+9210:15:Kontonummer existiert nicht'
```

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 36	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein

II.8.4 Datensegmente

◆ Beschreibung

Hier werden die Daten für die Kreditinstitutsrückmeldung (z.B. Kontoumsätze) eingestellt. Auf ein Kundensegment hin (z.B. „Dauerauftragsbestand abrufen“) können hier eine Vielzahl von Segmenten mit identischer Kennung (und somit identischem Format jedoch unterschiedlichem Inhalt) zurückgeliefert werden (z.B. jedes Segment liefert die Daten eines Dauerauftrags).



Falls das Kreditinstitut mehrere Versionen eines Geschäftsvorfalles unterstützt, hat es stets mit einem Segment derjenigen Version zu antworten, die dem Auftragssegment der Kundennachricht entspricht.

Beispiel: Wenn das Kreditinstitut die Versionen 2, 3 und 4 unterstützt und das Kundenprodukt sendet einen Abholauftrag mit der Segmentversion 3, so hat das Kreditinstitut ebenfalls ein Antwortsegment der Segmentversion 3 zurückzumelden.

◆ Format

Name: [Datensegmente](#)
Typ: [Segmentfolge](#)
Sender: Kreditinstitut

◆ Erläuterungen

Die Segmentfolge enthält die im Kapitel VII definierten Rückmeldungssegmente des Kreditinstituts. Jedes Segment kann dabei beliebig oft auftreten.

◆ Beispiel

```
HIKAZ:4:4:3+@362@<MT 940>+@102@<MT 942>'
HISAL:5:3:4+1234567:280:10020030+Giro Spezial+DE
M+C:1000,:DEM:19960701+D:500,:DEM:19960701+5000,
:DEM+7138,35:DEM+1476,98:DEM'
HIDAB:6:1:5+1234567:280:10020030+7654321:280:200
30040+MEIER FRANZ++1000,:DEM+52+000+MIETE:UND NE
BENKOSTEN+19960901+00001+19960701:M:1:1:19970601
+N:::3'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein	Stand: 02.02.1998	Seite: 37

II.8.5 RückmeldungsCodes

II.8.5.1 Grundkonzept

Die Änderung und Ergänzung von RückmeldungsCodes erfolgt in Abstimmung mit allen beteiligten Verbänden (Gewährleistung der Multibankfähigkeit). Änderungen bestehender Codes implizieren darüber hinaus neue Versionsnummern der betreffenden Segmentformate.

Institutsindividuelle Rückmeldungen (z.B. Konditionen, Werbung, Hinweise) sind über den Codebereich "Kreditinstitutsindividuelle Rückmeldung" zu generieren.

Pro Auftrag (Segment) darf vom Kreditinstitut nur eine Erfolgsmeldung, jedoch beliebig viele Warnungs- und Fehlermeldungen eingestellt werden.



Die RückmeldungsCodes sollen Kundensystemen automatisierte Reaktionen auf Institutsnachrichten ermöglichen; z.B. kann bei der Rückmeldung "BLZ falsch" das Kundensystem automatisiert zur Korrektur der BLZ aus einer hinterlegten BLZ-Tabelle auffordern.

Der „Rückmeldungstext“ dient dazu, den Kunden klartextliche Informationen zu übermitteln. Kundenprodukte sollten die kreditinstitutsseitigen Rückmeldungen im vollständigen Klartext anzeigen. Ebenso sollte der numerische Rückmeldungscode stets angezeigt werden, um den Kreditinstituten eine einfachere Bearbeitung von Kundenrückfragen zu spezifischen Rückmeldungstexten zu ermöglichen.

II.8.5.2 Rückmeldung

◆ Beschreibung

Die Codes beziehen sich auf unterschiedliche Datenstrukturen (Nachricht, Segment, DEG, DE etc.). In Bezug auf eine Datenstruktur können mehrere Codes zurückgeliefert werden.

Zu beachten:

Der Umfang der Online-Prüfung (z.B. nur physikalische Entgegennahme der Nachricht oder auch Syntax- und bankfachliche Prüfung) ist institutsindividuell.

◆ Format

Name: Rückmeldung
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Rückmeldungscode	GD	dig	4	M	1	
2	Bezugsdatenelement	GD	an	..7	K	1	
3	Rückmeldungstext	GD	an	..80	M	1	
4	Rückmeldungsparameter	GD	an	..35	K	10	

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 38	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein

♦ Erläuterungen

Nr. 1: Rückmeldungscode

Die erste Ziffer des Codes beschreibt die Meldungsklasse:

1. Ziffer	Meldungsklasse
0	Erfolg
3	Warnung
9	Fehler

Die zweite Ziffer des Codes beschreibt die Art der Meldung:

2. Ziffer	Meldungstyp
0	Meldungen zum Status
1	Meldungen zur Syntax
2	Geschäftsvorfallspezifische Meldungen
3	Meldungen zum Sicherungsverfahren
4	Meldungen zum Sicherungsmedium (reserviert)
8	Sonstige Meldungen
9	Kreditinstitutsindividuelle Meldungen

Die restlichen zwei Ziffern geben den Inhalt der Meldung an.

Nr. 2: Bezugsdatenelement

Falls sich der Rückmeldungscode auf ein Datenelement bzw. Gruppendatenelement bezieht, ist dessen Position anzugeben. So ist z.B. bei Syntaxfehlern die Position des fehlerhaften Elementes einzustellen. Bei Rückmeldecodes, die sich auf eine Nachricht oder ein Segment (Auftrag) beziehen, darf dieses DE nicht belegt werden.



Die Angabe des Bezugsdatenelements erlaubt u.U. eine automatische Reaktion des Kundenproduktes. So kann bspw. bei fehlerhaften Eingaben des Kunden direkt auf das betreffende Eingabefeld positioniert werden.

Die Referenzierung erfolgt

- bei DE durch die Position
- bei GD durch die Position der DEG und die Position des GD (die beiden Werte sind durch Komma getrennt)

Position des DE:

Position des DE = Anzahl der vorstehenden DE-Trennzeichen + 1.

Die Anzahl der vorstehenden DE-Trennzeichen ist gleich der Anzahl der vorstehenden DE + Anzahl der vorstehenden DEGs (GD sind nicht separat zu zählen, sondern gehen in die DEGs ein). Entwertete Pluszeichen sind nicht zu zählen.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein	Stand: 02.02.1998	Seite: 39

Position des GD innerhalb einer DEG:

Position des GD = Anzahl der vorstehenden GD-Trennzeichen innerhalb der DEG + 1

Beispiele:

Segmentkopf+DE+GD:GD:GD:GD+DE+GD:GD' : 4
Segmentkopf+DE+GD:GD:GD:GD+DE+GD:GD' : 3,4
Segmentkopf+DE+GD:GD:GD:GD+DE+GD:GD' : 5,2

Nr. 3: Rückmeldungstext

Rückmeldung im Klartext.



Der in die Rückmeldung einzustellende Text kann vom Kreditinstitut frei gewählt werden. So können diese Texte an individuelle Anforderungen der einzelnen Institute angepaßt werden, um z.B. institutsspezifische Besonderheiten zu berücksichtigen. Anstatt eines freidefinierten Textes kann das Institut auch den in der Spalte „Code-Bedeutung“ definierten Text einstellen. Es ist zu beachten, daß der einzustellende Text den Formatvorschriften entspricht.

Das Kreditinstitut hat den Rückmeldungstext in einer Form einzustellen, daß dieser unverändert im Kundenprodukt angezeigt werden kann. Insbesondere ist der Text in der vom Kunden mit dem Sprachkennzeichen gewählten Sprache und unter Berücksichtigung der jeweiligen landesspezifischen Besonderheiten (z.B. Formatierung des Datums) darzustellen.

Bei Syntaxfehlern ist es ausreichend, dem Kunden den Text „Syntaxfehler“ ohne weitere Erläuterung zurückzumelden, da der Fehler im Regelfall vom Kundenprodukt verursacht wurde und nicht von Kunden behoben werden kann.

Nr. 4: Rückmeldungsparameter

Parameter dienen dazu, die Art der Meldung weiter zu spezifizieren, um z.B. einen Fehler weiter eingrenzen zu können und eine automatische Reaktion des Kundenprodukts zu ermöglichen. Es dürfen nur die zum jeweiligen Rückmeldungscode angegebenen Parameter eingestellt werden (s.u.).

Es ist zu beachten, daß die einzustellenden Daten den Formatvorschriften entsprechen.

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 40	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein

II.8.5.3 Reaktionsvorschriften

Bei Erfolgsmeldungen (Klasse 0) wird die Nachricht bzw. der Auftrag stets angenommen. Warnungen (Klasse 3) sind Hinweise auf mögliche Fehler, die jedoch nicht zur Ablehnung führen. Bei Fehlermeldungen (Klasse 9) wird die zugehörige syntaktische Einheit (Auftrag bzw. Nachricht) abgelehnt.

Auch wenn einzelne Aufträge einer Nachricht inkorrekt sind, müssen andere korrekte Aufträge in derselben Nachricht vom Kreditinstitut ausgeführt werden. Dies gilt auch für Syntaxfehler, sofern dieser nur Auswirkungen auf einen einzigen Auftrag hat. D.h., bei Syntaxfehlern in administrativen Segmenten (Nachrichtenkopf, Signaturkopf etc.) ist stets die gesamte Nachricht abzulehnen.

Beispiel:

Code-Bedeutung	Reaktion
DE im Auftrag syntaktisch ungültig	Nachricht ok, Auftrag nicht ok
DE im Nachrichtenkopf syntaktisch ungültig	Nachricht nicht ok, Auftrag nicht ok
Unbekannter Nachrichtenaufbau	Nachricht nicht ok, Auftrag nicht ok

Verstöße gegen die syntaktischen Festlegungen in Kapitel II sind nicht zu tolerieren, sondern führen zur Ablehnung des Auftrags bzw. der Nachricht.

Eine Nachricht, die nicht als HBCI-Nachricht identifiziert werden kann (z.B. Segmentkennung des Nachrichtenkopfes kann nicht identifiziert werden), wird nicht mit einer Kreditinstitutsnachricht beantwortet. In diesem Fall darf das Kreditinstitut von sich aus die Transportverbindung beenden. Nachrichten, die gegen grundlegende HBCI-Aufbauvorschriften verstoßen, sind mit dem Rückmeldungscode 9110 „Unbekannter Aufbau“ zu beantworten.

Grundsätzlich werden dem Kunden alle auftretenden Meldungen mitgeteilt.

Ausnahmen:

- Tritt in einer Nachricht ein Fehler auf, der dazu führt, daß eine syntaktische Einheit (z.B. Nachricht, Segment, DEG) komplett ungültig ist oder nachfolgende Teile der syntaktischen Einheit ebenfalls fehlerhaft sind (Folgefehler), so kann die Bearbeitung der syntaktischen Einheit nach diesem Fehler abgebrochen werden.
- Zu nachgeordneten syntaktischen Einheiten brauchen keine Meldungen rückgemeldet werden, falls deren Code derselbe ist wie der der übergeordneten syntaktischen Einheit (Bsp.: Falls die Nachricht insgesamt fehlerfrei ist, brauchen für die einzelnen Segmente keine Erfolgsmeldungen rückgemeldet werden).



Wurde ein Auftrag abgelehnt, so ist darauf zu achten, daß nach der Fehlerbehebung bei einem eventuellen neuen Senden durch das Kundensystem die Nachricht neu aufgebaut wird, d.h. insbesondere eine neue Signatur eingestellt wird.

Bei Transaktionsaufträgen kann bei der institutsinternen Verarbeitung unter Umständen ein Fehler auftreten, bei dem für das rückmeldende System nicht ersichtlich ist, ob der Fehler vor oder nach der Verarbeitung des Auftrags aufgetreten ist. In diesem Fall wird dem Kundenprodukt der Rückmeldungscode 9000 „Status indiffe-

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein	Stand: 02.02.1998	Seite: 41

rent“ mitgeteilt. Das Kundenprodukt darf den Auftrag anschließend nicht erneut einreichen, da er eventuell doppelt verarbeitet wird. Statt dessen hat der Kunde den Status des Auftrags auf anderem Wege in Erfahrung zu bringen. Das Kundenprodukt sollte dem Kunden einen entsprechenden Hinweis geben.

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 42	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein

II.8.5.4 Code-Bedeutungen

II.8.5.4.1 Erfolgsmeldungen

Code	Code-Bedeutung	Bezug	Parameter	Anmerkungen	Beispiel
0010	Entgegengenommen	Nachricht Segment		Umfang der Prüfung ist institutsspezifisch. Mindestanforderung: physikalisch korrekt empfangen; Status ist nicht rechtsverbindlich.	Nachricht entgegengenommen Auftrag entgegengenommen Auftrag zur Ausführung weitergeleitet
0020	Ausgeführt	Segment		rechtsverbindlicher Abschluß der Verarbeitung	Auftrag ausgeführt
0100	Beendet	Dialog		Bestätigung der Dialogendenachricht des Kunden	Dialog beendet
0900-0999	Individuell	alle		Institutsindividuelle Rückmeldung	individuell

II.8.5.4.2 Warnungen und Hinweise

Code	Code-Bedeutung	Bezug	Parameter	Anmerkungen	Beispiel
3010	Nicht verfügbar	Segment			z.Zt. keine Börsenkurse abrufbar Keine neuen Einträge im Statusprotokoll Information wird zur Zeit nicht angeboten Wertpapierdatei ist bereits aktuell
3020	Korrigiert, da nicht mehr aktuell	Element	Neuer Inhalt		Bankleitzahl veraltet. Die neue BLZ lautet...
3030	Korrigiert, da ungültig	Element	Neuer Inhalt		Datum ist kein Buchungstag. Der Auftrag wird ausgeführt am...
3040	Es liegen weitere Informationen vor	Segment	Aufsetzpunkt	Wiederaufsetzen möglich (s. Kap. II.7.3)	Auftrag nur teilweise ausgeführt
3050	Nicht mehr aktuell. Wird noch ... Tage akzeptiert	Segment Element	Tage		Segmentversion ist veraltet. Bitte Kundenprodukt aktualisieren Öffentlicher Schlüssel des Kreditinstituts ist nicht mehr aktuell
3060	Teilweise liegen Warnungen/Hinweise vor	Nachricht		in einer Nachricht ist mindestens ein Auftrag mit Warnungen oder Hinweisen enthalten	
3810	Zusätzlich Datei abholen	alle	Dateiname		Aktualisierte BLZ-Datei liegt bereit
3900-3999	Individuell	alle	individuell	Institutsindividuelle Rückmeldung	individuell

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein	Stand: 02.02.1998	Seite: 43

II.8.5.4.3 Fehlermeldungen

Code	Code-Bedeutung	Bezug	Parameter	Anmerkungen	Beispiel
9000	Status indifferent	Segment		Institutsinterne Verarbeitung ist fehlerhaft. Es ist unklar, ob der Auftrag verarbeitet wurde	
9010	Verarbeitung nicht möglich	Nachricht Segment			Kundennachricht zu umfangreich Verarbeitungssystem nicht verfügbar Auftrag zur Zeit nicht änderbar Löschung eines Auftrags ist nicht mehr möglich, weil dessen Ausführung bereits eingeleitet wurde
9020	Antwort zu groß	Nachricht		Kundennachricht ok, aber Kreditinstitutsantwort kann intern nicht verarbeitet werden	Zu viele Tagesauszüge; Bereich eingrenzen
9030	Fehler bei Entschlüsselung	Nachricht			Falsches Verschlüsselungsverfahren oder -version
9040	Fehler bei Dekomprimierung	Nachricht			Falsches Komprimierungsverfahren oder -version
9050	Teilweise fehlerhaft	Nachricht		in einer Nachricht ist mindestens ein fehlerhafter Auftrag enthalten	
9110	Unbekannter Aufbau	Nachricht Segment		Ungültige Segmentreihenfolge	
9120	Nicht erwartet	Nachricht			Zwei Dialoginitialisierungen nacheinander oder Auftragsnachricht ohne Dialoginitialisierung
9130	Inhalt syntaktisch ungültig	Element		unerlaubte Zeichen oder falsches Format	Betrag ungültig Datum ungültig
9140	Inhalt zu lang	Element		Länge des Elements entspricht nicht den Formatvorgaben	Kontonr. hat zu viele Stellen
9145	Inhalt zu kurz	Element		Länge des Elements entspricht nicht den Formatvorgaben	BLZ hat zu wenige Stellen
9150	Belegung nicht erlaubt	Element			Ausführungsdatum bei Einzelüberweisung belegt
9160	Fehlt	Segment Element		Bezugs-DE wird nicht belegt, da nicht definiert	Signatur fehlt DE mit Status „Muß“ fehlt
9170	Tritt zu oft auf	Segment Element			Zu viele Signaturen Zu viele Verwendungszweckzeilen

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 44	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein

Code	Code-Bedeutung	Bezug	Parameter	Anmerkungen	Beispiel
9180	Wird nicht mehr akzeptiert	Segment Element			Segmentversion ist veraltet. Bitte Kundenprodukt aktualisieren Öffentlicher Schlüssel des Kreditinstituts ist nicht mehr aktuell
9210	Inhaltlich ungültig	Element		Syntax ok, aber Belegung falsch	Mindestzeitraum bis zum Ausführungstermin überschritten Datum ist kein Buchungstag unerlaubter Textschlüssel
9212	Inhalt zu groß	Element	Erlaubter Maximalwert	Numerisches Feld mit zu hohem Wert belegt	Betrag zu groß bei Euroüberweisung Betrag kann technisch nicht verarbeitet werden
9215	Inhalt zu klein	Element	Erlaubter Minimalwert	Numerisches Feld mit zu kleinem Wert belegt	0 als Überweisungsbetrag nicht erlaubt
9220	Einzelposition inhaltlich ungültig	Segment	Identifikationsnr.		Sammelauftrag abgelehnt, da fehlerhafter Einzelauftrag Nr. ...
9230	Unzureichendes Guthaben des Kontos	Segment			
9310	Elektronische Signatur noch nicht hinterlegt	Segment		Benutzer registriert, aber öffentlicher Schlüssel noch nicht an das Kreditinstitut geschickt.	
9320	Elektronische Signatur noch nicht freigeschaltet	Segment		Öffentlicher Schlüssel bereits an das Kreditinstitut geschickt, "Ini-Brief" jedoch noch nicht, oder das Kreditinstitut hat nach Erhalt des "Ini-Briefs" die EU noch nicht freigegeben.	
9330	Elektronische Signatur gesperrt	Segment		Gesamtspernung	
9340	Elektronische Signatur falsch	Segment			
9360	Sperrung der Signatur nach weiteren x Falschsignaturen	Segment	Anzahl		
9370	Signaturberechtigung reicht nicht aus	Segment		Zwei "B-Unterschriften" für "Und-Konten", die mindestens eine "A-Unterschrift" erfordern	Anzahl Signaturen nicht ausreichend
9380	Benutzer hat keine Auftragsberechtigung	Segment		Signatur der Dialoginitialisierung reicht nicht zum Versenden der Aufträge aus	
9390	Doppeleinreichung	Segment			

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein	Stand: 02.02.1998	Seite: 45

Code	Code-Bedeutung	Bezug	Parameter	Anmerkungen	Beispiel
9400	Allgemeiner Fehler des Sicherheitsmediums	Nachricht			Sicherheitsmedium unbekannt Sicherheitsmedium ungültig
9800	Abgebrochen	Dialog		Kreditinstitutsseitige Beendigung des Dialoges	
9900-9999	Individuell	alle	individuell	institutsindividuelle Rückmeldung	individuell

Kapitel: II	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 46	Stand: 02.02.1998	Kapitel: Nachrichtenaufbau Abschnitt: Allgemeiner Nachrichtenaufbau bei Verschlüsselung

II.9 Allgemeiner Nachrichtenaufbau bei Verschlüsselung

◆ Beschreibung

Es werden generell sowohl alle Kunden- als auch alle Kreditinstitutsnachrichten verschlüsselt. Ausnahmen sind in Kap. III.1.3 aufgeführt.

Für den Aufbau von verschlüsselten Nachrichten ist folgendes Vorgehen einzuhalten⁶:

1. Die Nachricht ist zunächst unverschlüsselt aufzubauen.
2. Das Segment „Verschlüsselungskopf“ ist direkt hinter dem Nachrichtenkopf einzustellen.
3. Die verschlüsselten Signatur- und Auftragssegmente sind in das Segment „Verschlüsselte Daten“ einzustellen.

Vor der Verschlüsselung weisen die Segmente eine kontinuierliche Numerierung auf (s. Abb. links). Um die Eindeutigkeit der Segmentnummern zu gewährleisten erhält das Segment „Verschlüsselungskopf“ die Segmentnummer 998 und das Segment „Verschlüsselte Daten“ die Segmentnummer 999 (s. Abb. rechts). Diese beiden Segmentnummern dürfen daher vor der Verschlüsselung noch nicht vergeben worden sein. Bei der Entschlüsselung wird das Segment „Verschlüsselungskopf“ entfernt und das Segment „Verschlüsselte Daten“ in die Einzelsegmente aufgelöst, so daß die Nachricht wieder eine kontinuierliche Segmentnumerierung aufweist.

Vor Verschlüsselung:

Nr.	Segmentname
1	Nachrichtenkopf
2	Signaturkopf
3	Auftrag 1
4	Auftrag 2
5	Signaturabschluß
6	Nachrichtenabschluß

Nach Verschlüsselung:

Nr.	Segmentname
1	Nachrichtenkopf
998	Verschlüsselungskopf
999	Verschlüsselte Daten (enthält: 2 Signaturkopf 3 Auftrag 1 4 Auftrag 2 5 Signaturabschluß)
6	Nachrichtenabschluß

◆ Format

Name: Verschlüsselte Nachricht
Typ: Nachricht
Sender: Kunde/Kreditinstitut

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Verschlüsselungskopf	SEG	HNVSK	M	1	s. Kap. VI.5.4
3	Verschlüsselte Daten	SEG	HNVSD	M	1	s. Kap. VI.5.5
4	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

⁶ Falls im Fortlauf dieses Dokuments Nachrichtenaufbautabellen dargestellt sind, wurde stets die unverschlüsselte Form (s.o.) gewählt.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: II
Kapitel: Nachrichtenaufbau Abschnitt: Allgemeiner Nachrichtenaufbau bei Verschlüsselung	Stand: 02.02.1998	Seite: 47

◆ Erläuterungen

Nr. 3: Verschlüsselte Daten

In dieses Segment sind die verschlüsselten Signatur- und Auftragssegmente einzustellen.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Inhaltsverzeichnis	Stand: 02.02.1998	Seite: 1

III. DIALOGSPEZIFIKATION

III.1 Allgemeines.....	3
III.1.1 Begriffsbestimmung.....	3
III.1.2 Dialogabfolge	6
III.1.3 Verschlüsselung der Dialoges	8
III.2 Abfolge von Operationen	9
III.3 Dialoginitialisierung.....	10
III.3.1 Kundennachricht	11
III.3.1.1 Nachrichtenformat.....	11
III.3.1.2 Segment: Identifikation	12
III.3.1.3 Segment: Verarbeitungsvorbereitung	14
III.3.1.4 Segment: Anforderung eines öffentlichen Schlüssels.....	16
III.3.2 Kreditinstitutsnachricht	17
III.3.2.1 Nachrichtenformat.....	17
III.3.2.2 Segmentfolge: Bankparameterdaten	18
III.3.2.3 Segmentfolge: Userparameterdaten	19
III.3.2.4 Segment: Übermittlung eines öffentlichen Schlüssels	20
III.3.2.5 Segment: Kreditinstitutsmeldung	21
III.4 Dialogbeendigung	23
III.4.1 Kundennachricht	23
III.4.1.1 Nachrichtenformat.....	23
III.4.1.2 Segment: Dialogende	24
III.4.2 Kreditinstitutsnachricht	24
III.5 Anonymer Zugang	25
III.5.1 Dialoginitialisierung.....	25
III.5.2 Auftragsnachricht	27
III.5.3 Dialogbeendigung	28
III.6 Verbindungsabbruch	29
III.7 Statusprotokoll	32
III.8 Synchronisierung	36
III.8.1 Kundennachricht	37
III.8.1.1 Nachrichtenformat.....	37
III.8.1.2 Segment: Synchronisierung	37
III.8.2 Kreditinstitutsnachricht	38
III.8.2.1 Nachrichtenformat.....	38
III.8.2.2 Segment: Synchronisierungsantwort.....	39

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Allgemeines	Stand: 02.02.1998	Seite: 3

III.1 Allgemeines

III.1.1 Begriffsbestimmung

Die Identifizierung des Kunden sowie die Festlegung der Rechte, die einem Kunden im Rahmen eines HBCI-Dialoges offenstehen, erfolgt in HBCI anhand der Begriffe 'Benutzer' und 'Kunde' bzw. anhand der zugeordneten Identifikationsmerkmale 'Benutzerkennung' und 'Kunden-ID'. Hierzu sind folgende Unterscheidungen zu treffen:

Benutzer

Ein Benutzer ist eine natürliche Person, die als Inhaber oder Berechtigter (z.B. Bevollmächtigter) eines Kontos über ein Kundenprodukt/-endgerät am HBCI-Verfahren teilnimmt. Jeder Benutzer kann von seinem Kreditinstitut Userparameterdaten erhalten, in denen er über seine Rechte im Rahmen des HBCI-Verfahrens informiert wird. Dem Kreditinstitut gegenüber tritt der Benutzer als Inhaber eines Sicherheitsmediums auf.

Benutzerkennung

Die Identifizierung des Benutzers erfolgt anhand der Benutzerkennung. Die Vergabe obliegt dem Kreditinstitut. Das Kreditinstitut hat zu gewährleisten, daß die Benutzerkennung institutsweit eindeutig ist. Sie kann beliebige Informationen enthalten, darf aber bei Verwendung des RDH-Verfahrens¹ aus Sicherheitsgründen nicht aus benutzer- oder kreditinstitutsspezifischen Merkmalen hergeleitet werden.

Kunde

Neben dem allgemeinen Gebrauch des Kundenbegriffs in Abgrenzung zum Kreditinstitut kann der Begriff 'Kunde' optional dazu verwendet werden, eine institutsindividuelle Differenzierung eines Benutzers zu ermöglichen, um die Rolle, in der er auftritt, zu spezifizieren. So läßt sich zum Beispiel unterscheiden, ob ein Benutzer den Dialog in der Eigenschaft als Privatperson oder als Bevollmächtigter einer Firma führen möchte (s. Abb. 4). Durch die Rolle werden die Rechte festgelegt, die dem Benutzer im HBCI-Dialog zur Verfügung stehen. Es steht dem Kreditinstitut frei, dem Benutzer für jede Rolle eine eigene Benutzerkennung (Sicherheitsmedium) zur Verfügung zu stellen.

Diese Rolle muß nicht zwingend über eine eigene Kunden-ID im HBCI-System festgelegt werden. Bei Gleichheit von Benutzerkennung und Kunden-ID im HBCI-System wird die Rolle des Kunden im nachgelagerten operativen System festgelegt. Sie entscheidet sich durch die Verknüpfungen zwischen Benutzerkennung und 'interner' Kundennummer und den dazugehörigen Konten mit ihren jeweiligen Vollmachten.

Der Kundenbezug gilt immer für den gesamten Dialogkontext, d.h. für sämtliche Benutzer, die im Rahmen des Dialoges als Signierende auftreten (d.h. auch für eventuelle Zweit- und Drittsignierende).

¹ s. Kap. VI

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 4	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Allgemeines

Kunden-ID

Die Identifizierung des 'Kunden' erfolgt anhand der Kunden-ID. Die Vergabe obliegt dem Kreditinstitut. Das Kreditinstitut hat zu gewährleisten, daß die Kunden-ID institutsweit eindeutig ist. Sie kann beliebige Informationen enthalten. Es steht dem Kreditinstitut frei, ob es jedem Kunden genau eine Kunden-ID zuordnet (wie in Abb. 5 gezeigt) oder dem Kunden in Abhängigkeit vom Benutzer jeweils eine unterschiedliche Kunden-ID zuordnet.



Da Kunden-ID und Benutzerkennung voneinander abweichen können, ist im Kundenprodukt eine Eingabemöglichkeit für die Kunden-ID vorzusehen.

Im einzelnen sind folgende Belegungsvarianten für Benutzerkennung und Kunden-ID möglich:

- Benutzerkennung und Kunden-ID sind identisch:

In diesem Fall wird institutsseitig keine logische Differenzierung zwischen Kunde und Benutzer vorgenommen. Die Benutzerkennung wird in das Feld 'Kunden-ID' eingestellt. Die Rolle des Benutzers ergibt sich, wie oben dargestellt, erst im nachgelagerten System.

- Benutzerkennung und Kunden-ID sind nicht identisch:

Es wird institutsseitig eine logische Differenzierung zwischen Kunde und Benutzer vorgenommen, um die Rolle festzulegen, in der der Benutzer auftritt.

Die folgenden Abbildungen gelten für den Fall, daß die Kunden-ID genutzt wird, um die Rolle des Benutzers festzulegen:

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Allgemeines	Stand: 02.02.1998	Seite: 5

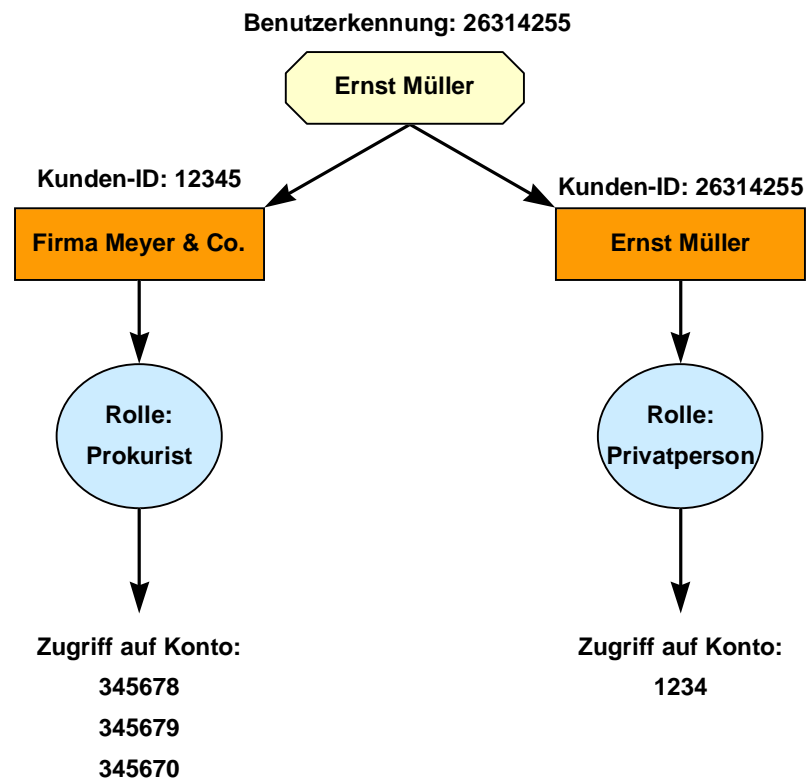


Abb. 4: Benutzer, mehreren Kunden zugeordnet

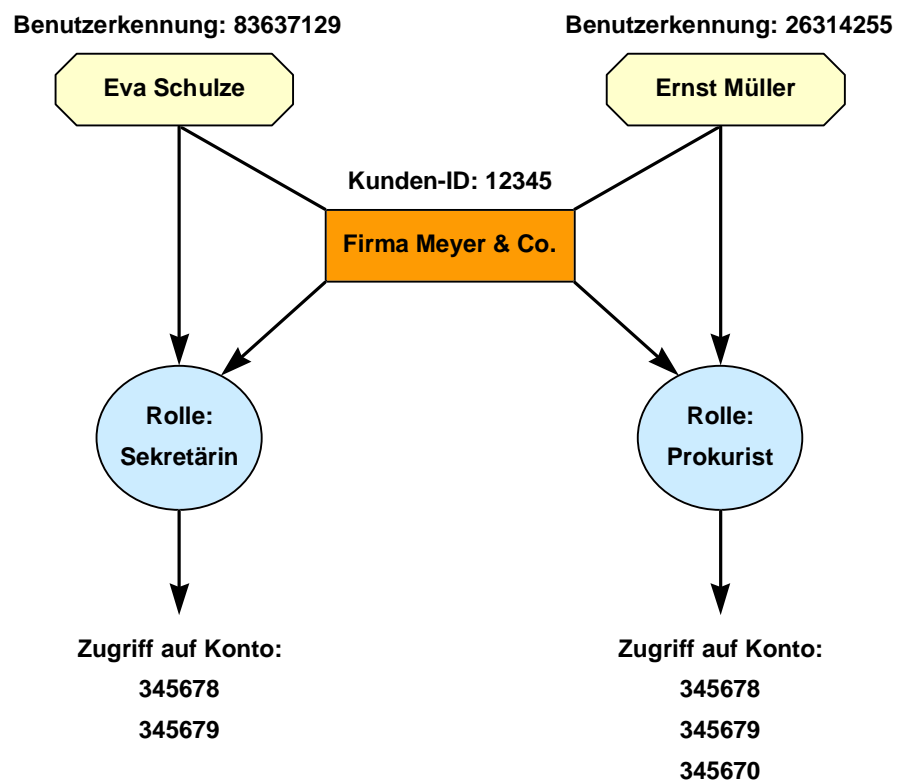


Abb. 5: Kunde, mehreren Benutzern zugeordnet

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 6	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Allgemeines

III.1.2 Dialogabfolge

Die Initiierung eines Dialogs geht stets vom Kunden aus. Auf eine Kundennachricht wird stets mit einer genau definierten Kreditinstitutsnachricht unmittelbar geantwortet. Erst wenn der Kunde diese Kreditinstitutsnachricht vollständig erhalten hat, darf er die nächste Nachricht an das Kreditinstitut übermitteln (Ausnahme: Nach einem Verbindungsabbruch sendet der Kunde im nächsten Dialog eine Nachricht an das Kreditinstitut, ohne vorher eine vollständige Antwortnachricht erhalten zu haben). Sowohl Kunde als auch Kreditinstitut dürfen jeweils nur eine Nachricht auf einmal übermitteln. Das Kundensystem hat die Pflicht, solange zu warten, bis das Kreditinstitut die entsprechende Antwortnachricht übermittelt hat.

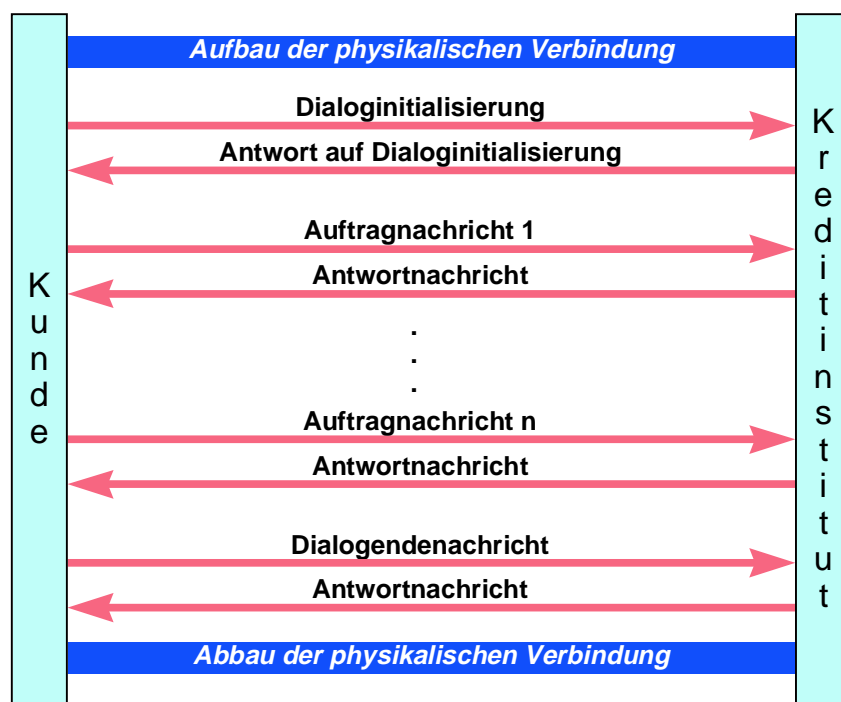


Abb. 6: Dialogabfolge

Jeder Dialog beginnt mit einer Dialoginitialisierungsnachricht. Erst wenn das Kundensystem die Bestätigungsnachricht erhalten hat, darf die erste Auftragsnachricht gesendet werden. Sollen keine weiteren Auftragsnachrichten mehr gesendet werden, so hat das Kundensystem eine Dialogendenachricht zu senden. Mit der Rückmeldung auf diese Nachricht erhält das Kundensystem die Dialogendebestätigung des Kreditinstituts.

Im Ausnahmefall kann das Kreditinstitut den Dialog auch von sich aus beenden (z.B. bei wiederholter ungültiger Authentisierung des Kunden). Hierzu sendet es in der Antwort auf eine Kundennachricht den Rückmeldungscode 9800 („Dialog abgebrochen“). Danach kann es die Transportverbindung abbauen. Das Kundenprodukt hat den Dialog in diesem Fall als beendet anzusehen und darf keine Dialogendenachricht mehr schicken.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Allgemeines	Stand: 02.02.1998	Seite: 7

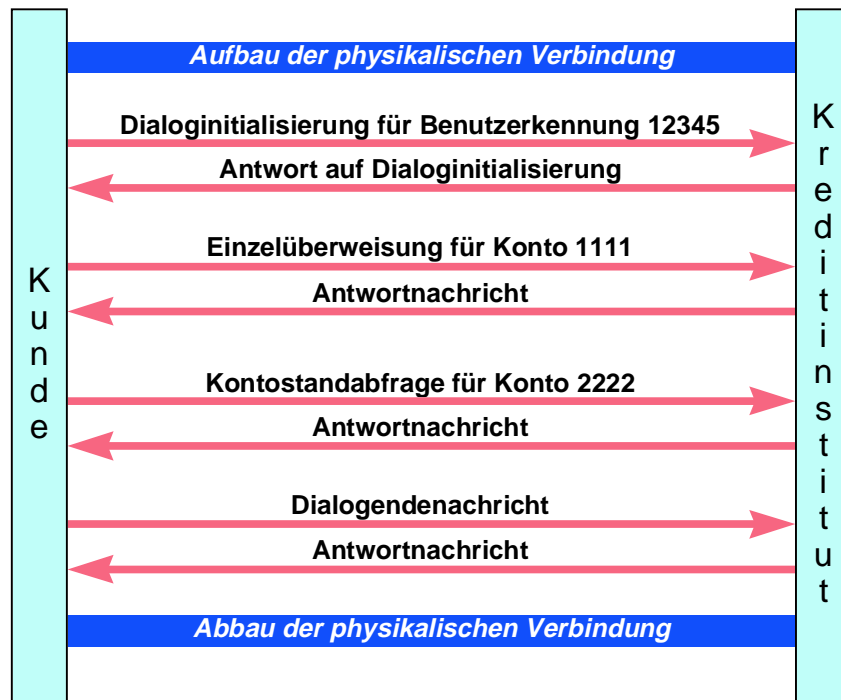


Abb. 7: Einzelbenutzer

Sollen Aufträge für mehrere Benutzer gesendet werden, ohne daß die physikalische Verbindung unterbrochen wird, so ist für jede neue Benutzerkennung eine neue Dialoginitialisierung durchzuführen (s. Abb. 8).

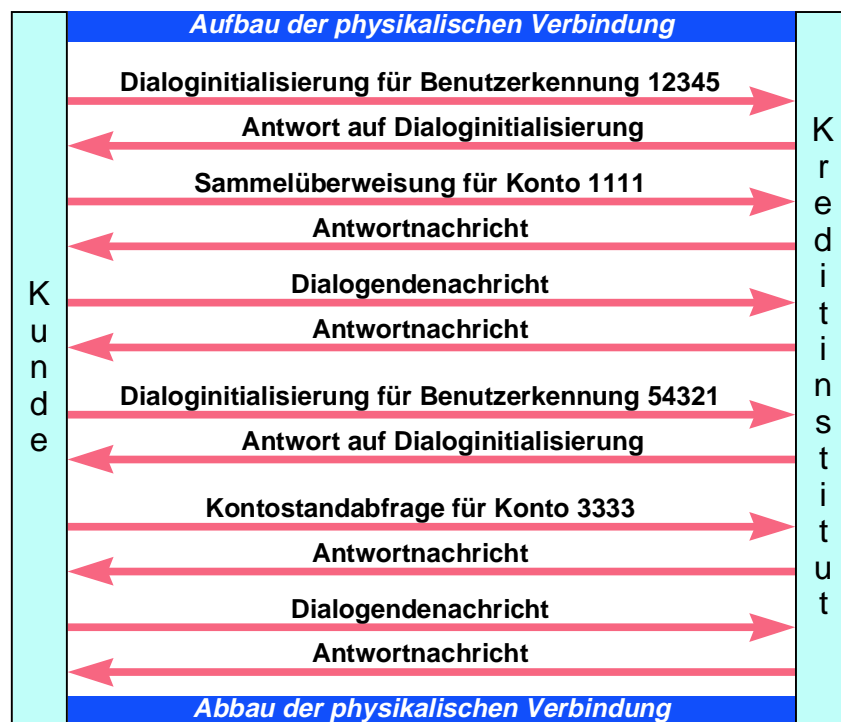


Abb. 8: Mehrere Benutzer

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 8	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Allgemeines

III.1.3 Verschlüsselung der Dialoges

Grundsätzlich sind sowohl alle Kunden- als auch alle Kreditinstitutsnachrichten eines Dialoges zu verschlüsseln. Von dieser Regel ausgenommen sind die folgenden Dialogarten:

- Anonymer Zugang (vgl. Kap. III.5)
- Erstmalige Anforderung der öffentlichen Schlüssel des Kreditinstituts (vgl. Kap. VI.6.2.2)
- Schlüsselsperrung durch den Kunden (vgl. Kap. VI.6.2.4)²
- Kommunikationszugang anfordern (VIII.7)



Unverschlüsselte Nachrichten, die keiner der oben genannten Ausnahmen zuzuordnen sind, sind vom empfangenden System abzulehnen.



Alle Kundennachrichten eines Dialoges sind vom Übermittler der Nachricht zu verschlüsseln. Alle Kreditinstitutsnachrichten sind mit dem öffentlichen Schlüssel des Übermittlers zu verschlüsseln.

Kunde und Kreditinstitut haben stets dasselbe Verschlüsselungsverfahren anzuwenden. Der Kunde gibt im Verschlüsselungskopf (Kap. VI.5.4) den von ihm verwendeten Verschlüsselungsalgorithmus an und bestimmt damit ebenfalls den Algorithmus, den das Kreditinstitut anzuwenden hat. Weder Kunde noch Kreditinstitut dürfen das Verfahren während des Dialoges wechseln. Der Kunde darf nur ein Verfahren wählen, das vom Kreditinstitut unterstützt wird. Die vom Kreditinstitut unterstützten Verfahren werden dem Kundensystem in den Bankparameterdaten im Segment „Sicherheitsverfahren“ (Kap. IV.4) bzw. Komprimierungsverfahren (Kap. IV.5) mitgeteilt.



Falls das Kreditinstitut das vom Kunden gewählte Verschlüsselungsverfahren nicht unterstützt, ist dem Kunden eine entsprechende Rückmeldung zu geben und der Dialog zu beenden. Das Kundenprodukt wird diese Nachricht nicht entschlüsseln können, da es das Verschlüsselungsverfahren des Kreditinstituts nicht unterstützt. Das Kundenprodukt hat in diesem Fall dem Verschlüsselungskopf der Kreditinstitutsnachricht zu entnehmen, daß es ein dem Kreditinstitut nicht bekanntes Verschlüsselungsverfahren verwendet. In diesem Fall hat der Kunde über den (unverschlüsselten) anonymen Zugang die aktuellen Bankparameterdaten anzufordern, in denen die Verschlüsselungsverfahren des Kreditinstituts angegeben sind.

² Es liegt im Ermessen des Kreditinstituts, ob es auch unverschlüsselte Sperren (z.B. aufgrund Schlüsselverlust des Kunden) entgegennimmt.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Abfolge von Operationen	Stand: 02.02.1998	Seite: 9

III.2 Abfolge von Operationen

Bei der Erstellung einer Nachricht sind die Arbeitsschritte in folgender Reihenfolge auszuführen (Arbeitsschritte teils optional):

1. Zusammenstellung der Informationen im System des Senders
2. Aufbau der Nachricht. Aus den Informationen werden die zu übertragenden Segmente bis auf ggf. erforderliche Signatur-Segmente aufgebaut, wobei beim Einstellen der Informationen in die Nachricht Syntaxzeichen entwertet werden.
3. Bildung der elektronischen Signatur (optional)
 - Erstellung des Signaturkopfes
 - Berechnung der elektronischen Signatur über Signaturkopf und Auftrags-segmente
 - Erstellung des Signaturabschlusses und Einstellung der Daten in das entsprechende Feld
4. Wiederholung von Schritt 3 für weitere Signaturen (optional)
5. Komprimierung (z.Zt. noch nicht zugelassen)
6. Verschlüsselung (Ausnahme: nicht verschlüsselungspflichtige Nachrichten)

Beim Empfänger einer Nachricht erfolgen die Verarbeitungsschritte entsprechend in umgekehrter Reihenfolge:

1. Entschlüsselung (Ausnahme: unverschlüsselte Nachrichten)
2. Dekomprimierung (z.Zt. noch nicht zugelassen)
3. Syntaxprüfung
4. Prüfung der elektronischen Signatur (optional)
 - Berechnung der elektronischen Signatur über Signaturkopf und Auftrags-segmente gemäß Parametern im Signaturkopf
 - Extrahieren des Signaturwertes aus dem Signaturabschluß
 - Vergleich des berechneten und des extrahierten Signaturwertes
5. Wiederholung von Schritt 4 für weitere Signaturen (optional)
6. Zerlegung der übrigen Datensegmente, dabei Entfernung von Entwertungs-zeichen
7. Bereitstellung der Informationen zur Verarbeitung im System des Empfängers

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 10	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Dialoginitialisierung

III.3 Dialoginitialisierung

Die Dialoginitialisierung dient folgenden Zwecken:

1. Prüfung, ob der Kommunikationspartner ein sendeberechtigter Benutzer ist
2. Festlegung der [Dialog-ID](#)
3. Prüfung auf Aktualität der im Kundensystem vorhandenen BPD und UPD sowie ggf. deren Aktualisierung
4. Prüfung auf Aktualität der öffentlichen Schlüssel des Kreditinstituts sowie ggf. deren Aktualisierung (nur bei asymmetrischen Verfahren)
5. Übermittlung vorbereitender Informationen für die kunden- und kreditinstituts-seitige Verarbeitung
6. Übertragung von Kreditinstitutsmeldungen

Während Auftragsnachrichten von dem bzw. den jeweiligen Signaturpflichtigen zu signieren sind, wird die Dialoginitialisierung von demjenigen Benutzer signiert, der sich im Rahmen der Dialoginitialisierung anmeldet. Im Regelfall ist dieser Benutzer auch Auftraggeber der nachfolgenden Aufträge, d.h. identisch mit dem Kunden. Während eines Dialoges dürfen nur Aufträge für Auftraggeberkonten gesendet werden, die der bei der Dialoginitialisierung angegebenen Kunden-ID zugeordnet sind.

Darüber hinaus darf die Dialoginitialisierung auch von einem Benutzer signiert werden, der für die nachfolgenden Auftraggeberkonten bevollmächtigt ist. Dies gilt auch bei Aufträgen für Konten mit Mehrfachunterschrift. Die Auftragsnachrichten müssen jedoch weiterhin von den Signaturpflichtigen signiert werden. Der Umfang der Bevollmächtigung ist Inhalt einer Vereinbarung zwischen Kunde und Kreditinstitut.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Dialoginitialisierung	Stand: 02.02.1998	Seite: 11

III.3.1 Kundennachricht

III.3.1.1 Nachrichtenformat

Realisierung Bank: verpflichtend

Realisierung Kunde: verpflichtend

◆ Beschreibung

Da der Kunde die Dialogsprache erst in dieser Nachricht mitteilt, muß zur Bildung der Dialoginitialisierungsnachricht der mit der Standardsprache des Kreditinstituts festgelegte Zeichensatz herangezogen werden. Dieser ist dem Feld „Standardsprache“ des Kommunikationszugangs zu entnehmen. Die Antwort des Kreditinstituts erfolgt dann in der vom Kunden gewünschten Sprache (Zeichensatz).

◆ Format

Name: Dialoginitialisierung

Typ: Nachricht

Sender: Kunde

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	M	1	s. Kap. VI.5.2
3	Identifikation	SEG	HKIDN	M	1	s. Kap. III.3.1.2
4	Verarbeitungsvorbereitung	SEG	HKVVB	M	1	s. Kap. III.3.1.3
5	Anforderung eines öffentlichen Schlüssels	SEG	HKISA	K	0-2	s. Kap. III.3.1.4
6	Signaturabschluß	SEG	HNSHA	M	1	s. Kap. VI.5.3
7	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

◆ Beispiel

s. Kap. VIII.5

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 12	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Dialoginitialisierung

III.3.1.2 Segment: Identifikation

◆ Beschreibung

Das Identifikations-Segment enthält Kontextinformationen, die für den gesamten Dialog Gültigkeit haben. Anhand dieser Daten wird die Sendeberechtigung des Benutzers geprüft. Eine Prüfung der transportmedienspezifischen Kennung des Benutzers erfolgt nicht.

Falls dem Benutzer die Berechtigung zum Senden weiterer Nachrichten nicht erteilt werden kann, ist ein entsprechender Rückmeldungscode in die Kreditinstitutsantwort einzustellen. Es steht Kreditinstituten frei, in bestimmten Fällen auf eine Identifizierung des Kunden zu verzichten. Dies ist zum Beispiel für den anonymen Zugang (s.u.) erforderlich, wo mit einem Nichtkunden kommuniziert wird.

◆ Format

Name: Identifikation
Typ: Segment
Segmentart: Administration
Kennung: HKIDN
Bezugssegment: -
Segmentversion: 2
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kreditinstitutskennung	DEG	kik	#	M	1	
3	Kunden-ID	DE	id	#	M	1	
4	Kundensystem-ID	DE	id	#	M	1	
5	Kundensystem-Status	DE	num	1	M	1	0,1

◆ Erläuterungen

Nr. 2: Kreditinstitutskennung

Es ist die Kennung des Kreditinstituts anzugeben, zu dem der Zugang gewünscht wird. In nachfolgenden Auftragsnachrichten dürfen nur Auftraggeberkonten dieses Institutbereichs angegeben werden.

Nr. 3: Kunden-ID

Es ist diejenige Kunden-ID des Benutzers einzustellen, die die Rolle festlegt, in der er im Rahmen des Dialoges auftritt (s. Kap. III.1.1). Diese Kunden-ID gilt ebenso für eventuelle Zweit- und Drittsignierende.

Nr. 4: Kundensystem-ID

Die Kundensystem-ID ist bei softwarebasierten Sicherheitsmedien erforderlich, wenn für einen Benutzer mehrere Signatur-IDs³ existieren (z.B. im Falle der Speicherung der Schlüsselpaare auf Festplatte). Die Kundensystem-ID

³ s. Kap. VI.5.2

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Dialoginitialisierung	Stand: 02.02.1998	Seite: 13

dient hier der eindeutigen Kennzeichnung des Kundensystems und sichert in Kombination mit der Signatur-ID die Validität (Eindeutigkeit) der Signatur.

Bei chipkartenbasierten Verfahren ist dieses DE mit dem Wert 0 zu belegen.



Bevor ein Benutzer bei Verwendung softwarebasierter Sicherheitsmedien von einem neuen Kundensystem Aufträge erteilen kann, hat er im Wege einer Synchronisierung (Kap. III.8) eine Kundensystem-ID für dieses System anzufordern. Diese ID ist im folgenden stets anzugeben, wenn der Benutzer von diesem Kundensystem aus Nachrichten sendet. Wenn eine Synchronisierung durchgeführt wird, ist die Kundensystem-ID mit dem Wert '0' zu belegen.

Kundensystem-IDs, die länger als 6 Monate nicht beim Kreditinstitut eingereicht wurden, können im Kreditinstitut gelöscht werden. Meldet sich der Kunde mit dieser Kundensystem-ID erneut an, wird keine Legitimierung zum Senden von Auftragsnachrichten erteilt. Der Kunde hat in diesem Fall eine erneute Synchronisierung durchzuführen.

Da jedes Kreditinstitut die Kundensystem-ID unabhängig von anderen Kreditinstituten vergibt, muß das Kundenprodukt in der Lage sein, für jeden Kreditinstitutszugang eine eigene Kundensystem-ID zu verwalten.

Nr. 5: Kundensystem-Status

Der Kundensystem-Status gibt an, ob die Kundensystem-ID erforderlich ist:

Code	Bedeutung
0	Kundensystem-ID wird nicht benötigt (chipkartenbasierte Sicherheitsmedien)
1	Kundensystem-ID wird benötigt (softwarebasierte Sicherheitsmedien)

♦ Beispiel

HKIDN:5:2+280:10020030+12345+2+1 '

♦ Ausgewählte Beispiele für Rückmeldungs-codes

Code	Beispiel für Rückmeldungstext
0020	Informationen fehlerfrei entgegengenommen
9210	Unbekannter Kunde
9210	Ungültige Kundensystem-ID

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 14	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Dialoginitialisierung

III.3.1.3 Segment: Verarbeitungsvorbereitung

◆ Beschreibung

Dieses Segment dient der Übermittlung von Informationen über das Kundensystem, mit Hilfe derer das Kreditinstitut individuell auf Anforderungen des Kunden reagieren kann.

◆ Format

Name: Verarbeitungsvorbereitung
Typ: Segment
Segmentart: Administration
Kennung: HKVVB
Bezugssegment: -
Segmentversion: 2
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	BPD-Version	DE	num	..3	M	1	
3	UPD-Version	DE	num	..3	M	1	
4	Dialogsprache	DE	num	..3	M	1	0,1,2,3
5	Produktbezeichnung	DE	an	..25	M	1	
6	Produktversion	DE	an	..5	M	1	

◆ Erläuterungen

Nr. 2: BPD-Version

Es ist die aktuelle Version der im Kundenprodukt vorliegenden BPD einzustellen. Falls noch keine BPD vorliegen, ist der Wert „0“ einzustellen. Anhand dieser Information prüft das Kreditinstitut, ob der Kunde über die aktuelle BPD-Version verfügt.

Nr. 3: UPD-Version

s. BPD-Version

Nr. 4: Dialogsprache

An dieser Stelle spezifiziert der Kunde die Sprache in der er im laufenden Dialog mit dem Kreditinstitut kommunizieren möchte. Rückmeldungen und Kreditinstitutsmeldungen werden (soweit kreditinstitutsseitig unterstützt) in der zuvor spezifizierten Sprache an den Kunden übermittelt. Damit verbunden wird ein zugehöriger HBCI-Basiszeichensatz (s. Kap. II.1), der sich durch einen ISO 8859-Codeset und einen ISO 8859-Subset definiert, ausgewählt. Die Definition des Subsets ist den Anlagen (Kap. VIII.4) zu entnehmen. Der Codeset soll ermöglichen, zu einem späteren Zeitpunkt evtl. auch nicht-lateinische Zeichensätze zuzulassen.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Dialoginitialisierung	Stand: 02.02.1998	Seite: 15

Gültig sind derzeit:

Sprachkennzeichen	Bedeutung	Sprachencode gemäß ISO 639	ISO 8859 Subset	ISO 8859 Codeset
1	Deutsch	de (German)	Deutsch	1 (Latin 1)
2	Englisch	en (English)	Englisch	1 (Latin 1)
3	Französisch	fr (French)	Französisch	1 (Latin 1)

Der Kunde darf lediglich ein Sprachkennzeichen einstellen, das im Rahmen der BPD vom Kreditinstitut an das Kundensystem übermittelt wurde.

Wenn noch keine BPD vorliegen, sollte das Kundensystem die Standardsprache des Instituts einstellen, die in der Kommunikationszugangsdatenbank mitgeteilt wird. Falls diese Datenbank nicht vorliegt, ist der Wert „0“ einstellen. Das Kreditinstitut antwortet in diesem Fall in seiner Standardsprache.

Nr. 5: Produktbezeichnung

Einzustellen ist der Name des Kundenproduktes, mit dem die Nachrichten erzeugt wurden. Diese Angabe dient dem Kreditinstitut, um Kundenprodukt-hersteller gezielt unterstützen zu können.

Nr. 6: Produktversion

Version des Kundenproduktes

♦ Beispiel

HKVVB:7:1+2+3+1+Homebanking Plus+3.0'

♦ Ausgewählte Beispiele für Rückmeldungs-codes

Code	Beispiel für Rückmeldungstext
0020	Informationen fehlerfrei entgegengenommen
3050	BPD nicht mehr aktuell. Aktuelle Version folgt
3050	UPD nicht mehr aktuell. Aktuelle Version folgt
9210	Sprache wird nicht unterstützt

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 16	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Dialoginitialisierung

III.3.1.4 Segment: Anforderung eines öffentlichen Schlüssels

◆ Beschreibung

Bei asymmetrischen Signatur- bzw. Verschlüsselungsverfahren muß dieses Segment zur Anforderung des öffentlichen Chiffrierschlüssels des Kreditinstituts eingestellt werden. Falls eine kreditinstitutsseitige Signierung der Nachrichten vorgesehen ist, muß dieses Segment zusätzlich auch zur Anforderung des öffentlichen Signierschlüssels eingestellt werden.

Bei symmetrischen Verfahren darf dieses Segment nicht eingestellt werden.

◆ Format

Name: Anforderung eines öffentlichen Schlüssels
Typ: Segment
Segmentart: Administration
Kennung: HKISA
Bezugssegment: -
Segmentversion: s. Kap. VI.6.1.2
Sender: Kunde
Format: s. Kap. VI.6.1.2

◆ Beispiel

s. Kap. VI.6.1.2

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel
0020	Angegebener Schlüssel ist noch aktuell
0020	Angegebener Schlüssel ist nicht mehr aktuell. Der neue Schlüssel wird mitgeteilt
9010	Sicherheitsverfahren unterstützt keine öffentlichen Schlüssel
9210	Angegebener Schlüssel ist im Kreditinstitut unbekannt

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Dialoginitialisierung	Stand: 02.02.1998	Seite: 17

III.3.2 Kreditinstitutsnachricht

III.3.2.1 Nachrichtenformat

Realisierung Bank: verpflichtend

Realisierung Kunde: verpflichtend

◆ Beschreibung

Sofern die Dialoginitialisierungsnachricht des Kunden fehlerhaft ist, darf die Kreditinstitutsnachricht nur dazu genutzt werden, dem Kunden die betreffenden Rückmeldecodes mitzuteilen. Es dürfen in diesem Fall keine Datensegmente (z.B. BPD, UPD) rückgemeldet werden.

◆ Format

Name: Antwort auf Dialoginitialisierung

Typ: Nachricht

Sender: Kreditinstitut

Nr.	Name	Typ	Ken-nung	Sta-tus	An-zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	K	1	s. Kap. VI.5.2
3	Rückmeldungen zur Gesamtnachricht	SEG	HIRMG	M	1	s. Kap. II.8.2
4	Rückmeldungen zu Segmenten	SEG	HIRMS	K	0..n	s. Kap. II.8.3
5	Bankparameterdaten	SF	#	K	1	s. Kap. III.3.2.2
6	Userparameterdaten	SF	#	K	1	s. Kap. III.3.2.3
7	Übermittlung eines öffentlichen Schlüssels	SEG	HIISA	K	0-2	s. Kap. III.3.2.4
8	Kreditinstitutsmeldung	SEG	HIKIM	K	0..n	s. Kap. III.3.2.5
9	Signaturabschluß	SEG	HNSHA	K	1	s. Kap. VI.5.3
10	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

◆ Beispiel

s. Kap. VIII.5

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 18	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Dialoginitialisierung

III.3.2.2 Segmentfolge: Bankparameterdaten

◆ Beschreibung

Entspricht die vom Kunden übermittelte BPD-Version nicht der aktuellen im Kreditinstitut gespeicherten Version, so erhält der Kunde automatisch die aktuellen Bankparameterdaten. Dies gilt auch, wenn ihm zu einem früheren Zeitpunkt bereits dieselben BPD gesendet wurden. Die BPD werden sofort aktiv, d.h. sie sollten dann vom Kundenprodukt unmittelbar verwendet werden.

Die Bankparameterdaten müssen stets komplett übertragen werden, d.h. das Auslassen einzelner Segmente ist nicht zulässig. Zu einem späteren Zeitpunkt ist denkbar, daß nur die geänderten BPD-Segmente übertragen werden.

◆ Format

Name: Bankparameterdaten
Typ: Segmentfolge
Sender: Kreditinstitut
Format: s. Kap. IV „Bankparameterdaten“

◆ Beispiel

s. Kap. IV „Bankparameterdaten“

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Dialoginitialisierung	Stand: 02.02.1998	Seite: 19

III.3.2.3 Segmentfolge: Userparameterdaten

◆ Beschreibung

Entspricht die vom Kunden übermittelte UPD-Version nicht der aktuellen im Kreditinstitut gespeicherten Version, so erhält der Kunde automatisch die aktuellen Userparameterdaten. Dies gilt auch, wenn ihm zu einem früheren Zeitpunkt bereits dieselben UPD gesendet wurden. Die UPD werden sofort aktiv, d.h. sie sollten dann vom Kundenprodukt unmittelbar verwendet werden.

Die Userparameterdaten müssen stets komplett übertragen werden, d.h. das Auslassen einzelner Segmente ist nicht zulässig. Zu einem späteren Zeitpunkt ist denkbar, daß nur die geänderten UPD-Segmente übertragen werden.



Es ist zu beachten, daß lediglich die Userparameterdaten des sich anmeldenden Benutzers aktualisiert werden. Falls mehrere Benutzer an der Erstellung der Aufträge beteiligt sind (z.B. bei Mehrfachsignaturen), so ist sicherzustellen, daß auch für die passiven Benutzer, die die Aufträge nicht versenden, sondern lediglich signieren, stets die aktuellen UPD vorliegen.

Hierzu haben sich die passiven Benutzer in regelmäßigen Abständen beim Kreditinstitut mit einer Dialoginitialisierung anzumelden, damit ggf. ihre Userparameterdaten aktualisiert werden können. Dieses Verfahren kann vom Kundenprodukt durch eine automatische Aufforderung unterstützt werden.

◆ Format

Name: Userparameterdaten
 Typ: Segmentfolge
 Sender: Kreditinstitut
 Format: s. Kap. V „Userparameterdaten“

◆ Beispiel

s. Kap. V „Userparameterdaten“

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 20	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Dialoginitialisierung

III.3.2.4 Segment: Übermittlung eines öffentlichen Schlüssels

◆ Beschreibung

Falls bei asymmetrischen Signatur- bzw. Verschlüsselungsverfahren einer der öffentlichen Schlüssel des Kreditinstituts aktualisiert wurde, wird dem Kunden dieser in diesem Segment zurückgemeldet. Das Segment kann sowohl für den Signierschlüssel als auch für den Chiffrierschlüssel eingestellt werden. Hat sich der jeweilige Schlüssel nicht geändert, so wird das Segment nicht gesendet.

Zur Verifizierung der Richtigkeit des öffentlichen Schlüssels muß entweder die Dialoginitialisierungs-Antwortnachricht signiert sein oder es muß auf alternativem Weg (z.B. Brief) ein neuer Hashwert übermittelt werden.

Bei symmetrischen Verfahren darf dieses Segment nicht eingestellt werden.

◆ Format

Name:	Übermittlung eines öffentlichen Schlüssels
Typ:	Segment
Segmentart:	Administration
Kennung:	HIISA
Bezugssegment:	HKISA
Segmentversion:	s. Kap. VI.6.1.3
Sender:	Kreditinstitut
Format:	s. Kap. VI.6.1.3

◆ Beispiel

s. Kap. VI.6.1.3

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Dialoginitialisierung	Stand: 02.02.1998	Seite: 21

III.3.2.5 Segment: Kreditinstitutsmeldung

◆ Beschreibung

Kreditinstitutsmeldungen können z.B. Werbenachrichten oder auch kundenrelevante Informationen zu Geschäftsvorfällen, die nicht in RückmeldungsCodes abgebildet werden können, beinhalten. Diese werden dem Kunden automatisch im Rahmen der Dialoginitialisierungsantwortnachricht übermittelt. Dadurch wird gewährleistet, daß die Zustellung dieser Meldungen nicht auf Initiative des Kunden erfolgen muß.

Zum jetzigen Zeitpunkt ist lediglich die Übermittlung von unformatierten Textnachrichten möglich. Zukünftig ist denkbar, daß die Meldungen auch formatierten Text und Multimediaobjekte (Grafiken etc.) enthalten.



Kreditinstitutsmeldungen können dem Kunden unmittelbar nach Erhalt, d.h. z.B. während im Hintergrund der Dialog abläuft, angezeigt werden.

Hersteller von Kundenprodukten sollten darüber hinaus eine Möglichkeit zur Verwaltung von Kreditinstitutsmeldungen vorsehen. Falls mehrere Meldungen gleichzeitig vorliegen, sollte der Kunde die Möglichkeit haben, die Meldungen nacheinander zu bearbeiten (Funktionen „Nächste lesen“, „Vorherige lesen“). Ferner sollten Kreditinstitutsmeldungen gespeichert, gelöscht und ausgedruckt werden können.

◆ Format

Name: Kreditinstitutsmeldung
Typ: Segment
Segmentart: Administration
Kennung: HIKIM
Bezugssegment: -
Segmentversion: 2
Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Betreff	DE	an	..35	M	1	
3	Freitextmeldung	DE	txt	.. 2048	M	1	

◆ Erläuterungen

Nr. 2: Betreff

Es ist das Thema der Meldung einzustellen.

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 22	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Dialoginitialisierung

Nr. 3: Freitextmeldung

Meldung im Klartext. Die Daten dürfen nicht um führende oder nachfolgende Leerzeichen gekürzt werden.

◆ Beispiel

```
HIKIM:10:2+ec-Karte+Ihre neue ec-Karte liegt zur
Abholung bereit.'
HIKIM:11:2+Dispokredit+Ihr Dispokredit wurde auf
5.000 DM erhöht.'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Dialogbeendigung	Stand: 02.02.1998	Seite: 23

III.4 Dialogbeendigung

Jeder Dialog ist durch eine Dialogendenachricht zu beenden. Das Senden der Dialogbeendigung hat zwei Funktionen: Zum einen teilt der Kunde mit, daß keine weiteren Nachrichten folgen und die Verbindung zum Kreditinstitut beendet werden soll. Zum anderen bestätigt der Kunde hiermit implizit den Erhalt aller vorangegangenen Kreditinstitutsnachrichten des Dialoges.

Nach Erhalt der Kreditinstitutsantwortnachricht ist der Dialog logisch beendet. Anschließend muß das Kundenprodukt entweder die Kommunikation physisch beenden oder einen neuen Dialog beginnen. Falls der Kunde keine Dialogbeendigung sendet, wird der Dialog kreditinstitutsseitig nach einem transportmedienabhängigen Timeout beendet.

Der Dialog kann auch bereits direkt nach der Dialoginitialisierung beendet werden, sofern der Kunde bspw. lediglich seine BPD und UPD aktualisieren möchte.

Realisierung Bank: verpflichtend

Realisierung Kunde: verpflichtend

III.4.1 Kundennachricht

III.4.1.1 Nachrichtenformat

◆ Beschreibung

Die Nachricht muß signiert und verschlüsselt werden (Ausnahmen s. Kap. III.1.3) und wird mit einer Standard-Kreditinstitutsnachricht beantwortet. Die Nachricht ist von demjenigen Benutzer zu signieren, der auch die Dialoginitialisierung signiert hat.

◆ Format

Name: Dialogbeendigung

Typ: Nachricht

Sender: Kunde

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	M	1	s. Kap. VI.5.2
3	Dialogende	SEG	HKEND	M	1	s. Kap. III.4.1.2
4	Signaturabschluß	SEG	HNSHA	M	1	s. Kap. VI.5.3
5	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 24	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Dialogbeendigung

III.4.1.2 Segment: Dialogende

◆ Format

Name: Dialogende
 Typ: Segment
 Segmentart: Administration
 Kennung: HKEND
 Bezugssegment: -
 Segmentversion: 1
 Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Dialog-ID	DE	id	#	M	1	

◆ Erläuterungen

Nr. 2: Dialog-ID

Es ist die Dialog-ID des zu beendenden Dialoges einzustellen (s. Kap. II.6.2).

◆ Beispiel

HKEND:11:1+4711'

III.4.2 Kreditinstitutsnachricht

◆ Beschreibung

Das Kreditinstitut bestätigt die Dialogbeendigung mit dem Rückmeldungscode 0100 („Dialog beendet“).

◆ Format

Name: Kreditinstitutsnachricht allgemein
 Typ: Nachricht
 Format: Kap. II.8.1

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0100	Dialog beendet

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Anonymer Zugang	Stand: 02.02.1998	Seite: 25

III.5 Anonymer Zugang

Um Kunden die Möglichkeit zu geben, sich anonym anzumelden, um sich bspw. über die angebotenen Geschäftsvorfälle fremder Kreditinstitute (von denen sie keine BPD besitzen) zu informieren bzw. nicht-signierungspflichtige Aufträge bei fremden Kreditinstituten einreichen zu können, kann sich der Kunde anonym (als Gast) anmelden.

Die Zugangsdaten zu den Fremdinstituten erhält der Kunde über den Abruf der Kommunikationszugänge (s. Anlagen).

Bei anonymen Dialogen werden Nachrichten weder signiert, noch können sie verschlüsselt und komprimiert werden.

Realisierung Bank: optional

Realisierung Kunde: optional

III.5.1 Dialoginitialisierung

a) Kundennachricht

◆ Format

Name: Dialoginitialisierung bei anonymem Zugang

Typ: Nachricht

Sender: Kunde

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Identifikation	SEG	HKIDN	M	1	s. Kap. III.3.1.2
3	Verarbeitungsvorbereitung	SEG	HKVVB	M	1	s. Kap. III.3.1.3
4	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

◆ Erläuterungen

Nr. 2: Identifikation

Die Datenelemente des Identifikationssegments sind wie folgt zu belegen:

- Kreditinstitutskennung: Ländercode und BLZ des gewünschten Instituts
- Kunden-ID: 9999999999⁴
- Kundensystem-ID: 0
- Kundensystem-Status: 0

Nr. 3: Verarbeitungsvorbereitung

Mit diesem Segment fordert der Kunde die Bankparameterdaten des Kreditinstituts an.

⁴ Diese Kunden-ID darf daher nicht an Kunden vergeben werden.

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 26	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Anonymer Zugang

Sofern schon von einem früheren anonymen Zugang Bank- oder Userparameterdaten dieses Kreditinstituts vorliegen, ist die jeweilige Versionsnummer anzugeben.

b) Kreditinstitutsnachricht

◆ Format

Name: Antwort auf [anonyme](#) Dialoginitialisierung
Typ: Nachricht
Sender: Kreditinstitut

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Rückmeldungen zur Gesamtnachricht	SEG	HIRMG	M	1	s. Kap. II.8.2
3	Rückmeldungen zu Segmenten	SEG	HIRMS	K	0..n	s. Kap. II.8.3
4	Bankparameterdaten	SF	#	K	1	s. Kap. III.3.2.2
5	Userparameterdaten	SF	#	K	1	s. Kap. III.3.2.3
6	Kreditinstitutsmeldung	SEG	HIKIM	K	0..n	s. Kap. III.3.2.5
7	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

◆ Erläuterungen

Nr. 4: Bankparameterdaten

Die BPD bei einem anonymen Zugang sind identisch mit denen bei einem Zugang als Kunde.

Nr. 5: Userparameterdaten

In den Gast-UPD sind im DE „Erlaubte Geschäftsvorfälle“ diejenigen Geschäftsvorfälle aufgeführt, die der Gast ausführen darf. Dies können jedoch nur Geschäftsvorfälle sein, für die keine Signatur erforderlich ist, wie z.B. der Abruf von Börsenkursen oder die Sendung einer Gastmeldung (Die Festlegung, für welche Geschäftsvorfälle eine Signatur erforderlich ist, ist institutsspezifisch).

Nr. 6: Kreditinstitutsmeldung

Bei den Meldungen kann es sich lediglich um allgemeine, d.h. nicht benutzerspezifische Informationen handeln.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Anonymer Zugang	Stand: 02.02.1998	Seite: 27

III.5.2 Auftragsnachricht

a) Kundennachricht

◆ Format

Name: Kundennachricht allgemein bei anonymem Zugang
Typ: Nachricht
Sender: Kunde

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Aufträge	SF	#	K	1	s. Kap. II.7.2
3	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

◆ Erläuterungen

Nr. 2: Aufträge

Es dürfen lediglich nicht-signierungspflichtige Geschäftsvorfälle (z.B. Abruf von Börsenkursen, Gastmeldung) eingestellt werden. Welche Geschäftsvorfälle signierungspflichtig sind, bestimmt das Kreditinstitut in der UPD des Kunden.

Die Auftraggeberkontonummer ist jeweils mit dem Wert „9999999999“ zu belegen:

b) Kreditinstitutsnachricht

◆ Format

Name: Kreditinstitutsnachricht allgemein
Typ: Nachricht
Format: s. Kap. II.8.1

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 28	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Anonymer Zugang

III.5.3 Dialogbeendigung

a) Kundennachricht

◆ Format

Name: Dialogbeendigung bei anonymem Zugang
Typ: Nachricht
Sender: Kunde

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Dialogende	SEG	HKEND	M	1	s. Kap. III.4.1.2
3	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

b) Kreditinstitutsnachricht

◆ Format

Name: Kreditinstitutsnachricht allgemein
Typ: Nachricht
Format: s. Kap. II.8.1

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

◆ Ausgewählte Beispiele für Rückmeldungs-codes

Code	Beispiel für Rückmeldungstext
0100	Dialog beendet

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Verbindungsabbruch	Stand: 02.02.1998	Seite: 29

III.6 Verbindungsabbruch

Im Unterschied zu einigen derzeit aktuellen Transportmedien erfolgt in keinem Fall kreditinstitutsseitig ein Abbruch der Übertragung von Kundennachrichten; auch dann nicht, wenn kreditinstitutsseitig bereits ein Fehler in der Nachricht während der Übertragung festgestellt wird. Der Abbruch wird aus Gründen der Einheitlichkeit nicht durchgeführt, weil entsprechende Funktionalitäten nicht bei allen Kommunikationsdiensten zur Verfügung stehen.

Bzgl. Verbindungsstörungen bzw. Abbrüchen sind aus Sicht des Kreditinstituts folgende Fälle zu unterscheiden:

Fall 1: Abbruch während der Kunde eine Dialoginitialisierung an das Kreditinstitut sendet

Der Kunde konnte in diesem Fall nicht identifiziert werden. Die Legitimation konnte demgemäß nicht erteilt werden.

Fall 2: Abbruch nachdem der Kunde eine Dialoginitialisierung an das Kreditinstitut gesendet hat

Die Nachricht wurde erhalten. Anschließend wurde der Kunde identifiziert und die Legitimation erteilt. Das Kreditinstitut erwartet eine Auftragsnachricht. Diese kann jedoch nicht eintreffen, da der Kunde die Antwortnachricht nicht erhalten hat.

Fall 3: Abbruch während der Kunde eine Auftragsnachricht an das Kreditinstitut sendet

In diesem Fall ignoriert das Kreditinstitut das erhaltene Nachrichtenfragment.

Fall 4: Abbruch nachdem der Kunde eine Auftragsnachricht an das Kreditinstitut gesendet hat

Der Abbruch erfolgt hierbei bevor oder während das Kreditinstitut die Antwortnachricht an den Kunden sendet. In diesem Fall wird die erhaltene Nachricht vom Kreditinstitut bearbeitet.

Bei einem Abbruch konnte der Dialog nicht ordnungsgemäß beendet werden. So fehlt z.B. die ordnungsgemäße Dialogbeendigung oder es fehlen bei einem Abbruch während der Dialoginitialisierung die Auftragsnachrichten. Das Kreditinstitut hat dennoch den Dialog als abgeschlossen zu betrachten, da der Kunde einen neuen Dialog beginnen muß, um sich über den Status der abgebrochenen Nachricht zu informieren.



Verhalten auf Kundenseite:

Erfolgt der Abbruch während oder nach der Dialoginitialisierung (Fall 1 und 2), ist der Dialog auf jeden Fall mit einer erneuten Dialoginitialisierung zu beginnen.

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 30	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Verbindungsabbruch

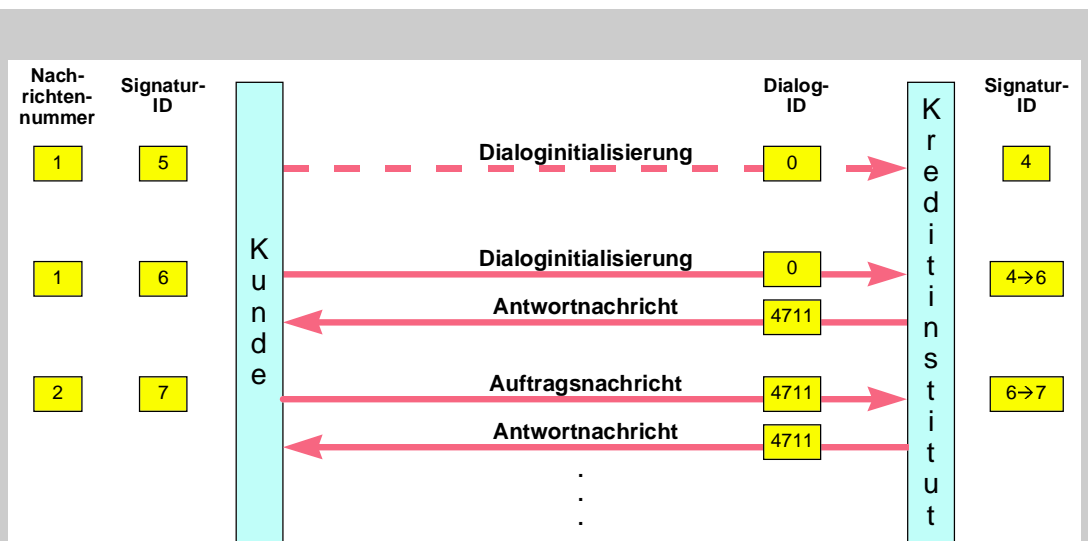


Abb. 9: Verbindungsabbruch Fall 1

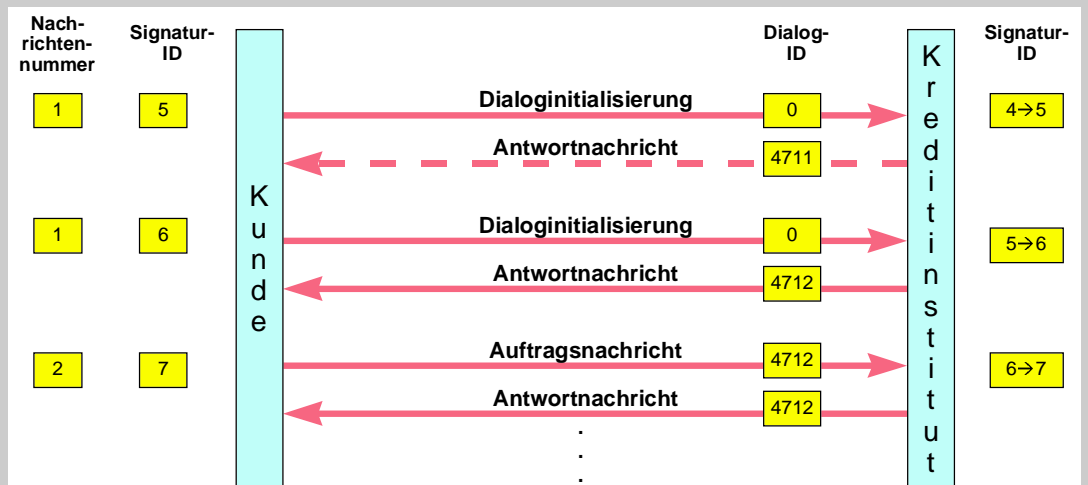


Abb. 10: Verbindungsabbruch Fall 2

Im Falle eines Abbruch während oder nach dem Senden einer Auftragsnachricht (Fall 3 und 4) ist für das Kundenprodukt im Regelfall nicht nachvollziehbar, zu welchem dieser beiden Zeitpunkte der Abbruch erfolgt ist. Dieses Kenntnis ist jedoch erforderlich, um zu entscheiden, ob die Auftragsnachricht erneut gesendet werden muß.

Das Kundenprodukt sendet hierzu eine **Synchronisierungsnachricht**. In der Antwortnachricht erhält es die letzte Nachrichtennummer der Kundennachricht, die im abgebrochenen Dialog noch verarbeitet wurde. Anhand dieser Information ist für das Kundenprodukt ersichtlich, welche Auftragsnachrichten noch gesendet werden müssen.

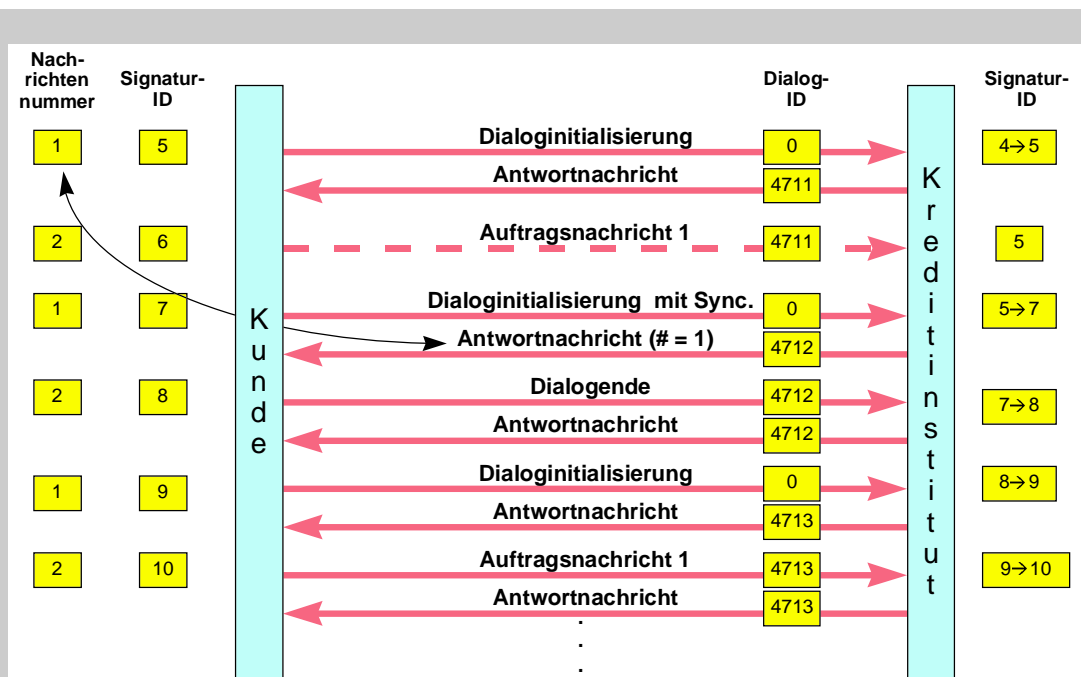


Abb. 11: Verbindungsabbruch Fall 3

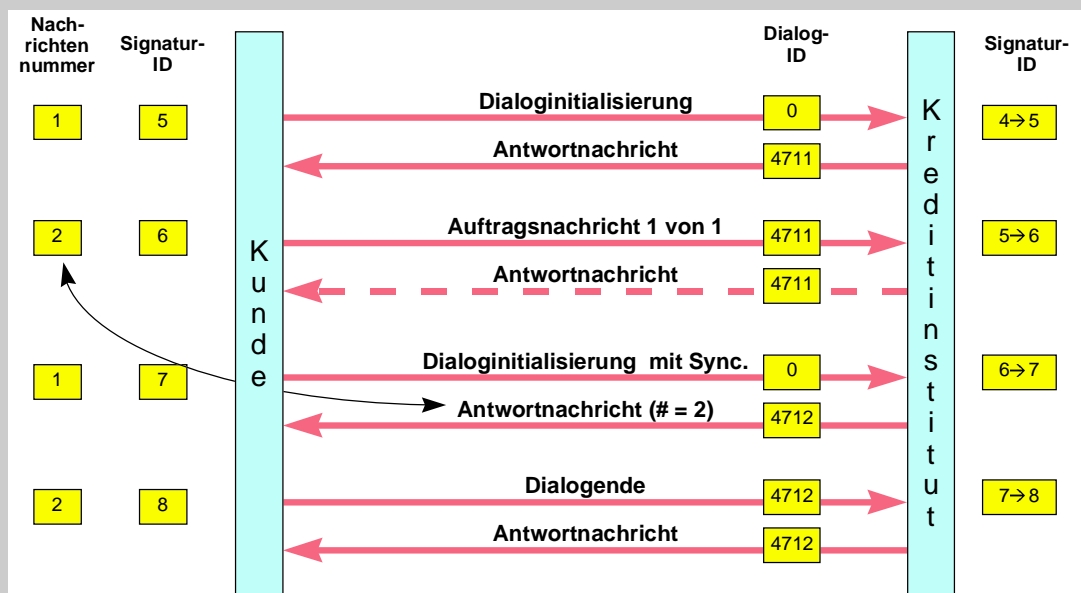


Abb. 12: Verbindungsabbruch Fall 4

Eine erneut zu sendende Nachricht darf nicht unverändert (bitidentisch) gesendet werden, da sie aufgrund der nicht mehr aktuellen Signatur-ID (s. Kap. VI.5.2) als Doppeleinreichung abgelehnt würde. Daher muß diese Nachricht im Signaturkopf und -abschluß eine neue Signatur-ID und folglich auch eine neue elektronische Signatur erhalten.

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 32	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Statusprotokoll

III.7 Statusprotokoll

Um dem Kunden bzw. dem Kundensystem die Möglichkeit zu geben, den Verarbeitungsstatus von Nachrichten abzufragen, wird kreditinstitutsseitig ein Statusprotokoll geführt, in dem die Stati aller Aufträge aufgeführt sind.

Dies ist beispielsweise sinnvoll, um Kunden die Ausführung ihrer Aufträge mitzuteilen, da online im Regelfall lediglich der Empfang der Aufträge bestätigt werden kann und die weitere Verarbeitung offline erfolgt. Ferner dient das Statusprotokoll dazu, nach einem Verbindungsabbruch den Status der übermittelten Aufträge zu erfahren, insbesondere wenn durch das Kundensystem eine Nachricht vollständig an das Kreditinstitut übermittelt wurde, beim Senden der Antwort seitens des Kreditinstituts jedoch ein Fehler auftrat.

Grundsätzlich erzeugen sämtliche als Geschäftsvorfall gekennzeichneten Segmente von Kundennachrichten (s. Kap. VIII.1 „Übersicht der Segmentkennungen“) einen Eintrag in das Statusprotokoll. Beim anonymen Zugang (s.o.) wird kein Statusprotokoll erzeugt.

Meldungen im Statusprotokoll sind identisch mit den Rückmeldungen zu Aufträgen in Kreditinstitutsnachrichten (s. Segment HIRMS). Daher kann ein Auftrag im Statusprotokoll durch 1 bis n Segmente beschrieben sein. Das Statusprotokoll enthält jeweils die letzte für den Kunden bestimmte(n) Rückmeldung(en) in Bezug auf einen Auftrag bzw. eine Rückmeldung, die den Abschluß der Bearbeitung beschreibt. Somit ist zu jedem Zeitpunkt der Verarbeitungsstatus eines Auftrages durch genau einen Status definiert. Ferner enthält das Statusprotokoll sämtliche Meldungen, die in das Segment „Rückmeldungen zur Gesamtnachricht“ (HIRMG) eingestellt werden.

Die Festlegung, welcher Teil der Rückmeldungen im Rahmen der Online-Prüfung (z.B. „Auftrag entgegengenommen“) und welcher Teil durch die Offline-Prüfung (z.B. „Auftrag ausgeführt“) generiert wird, ist kreditinstitutspezifisch.

Da Meldungen, die erst bei der Weiterverarbeitung generiert werden, identisch mit den Online-Meldungen sind, kann das Kundenprodukt auch bei asynchroner Verarbeitung wie beim Onlinebetrieb auf Meldungen des Kreditinstituts reagieren.

Statusmeldungen werden stets dem Absender des Auftrags zugeordnet, d.h. Stati sind benutzerbezogen und nicht kontenbezogen.

Die Frage, wie detailliert der Kunde über das Fortschreiten der kreditinstituts-internen Verarbeitung informiert werden soll, wird institutsindividuell gehandhabt.

Stati müssen im Protokoll als Abgleichhilfe mindestens bis zum Ablauf von 2 Buchungstagen nach dem nächsten Dialog, jedoch höchstens 6 Monate, vorgehalten werden. Auf diese Weise ist sichergestellt, daß dem Kunden keine Statusmeldungen verloren gehen (z.B. bei längerem Urlaub etc.). Gleichzeitig wird das kreditinstitutsseitig vorzuhaltende Datenvolumen minimiert, indem die Stati bereits 2 Tage nach dem nächsten Dialog gelöscht werden können.



Das Kundenprodukt sollte über ein Journal verfügen, in das sämtliche Statusmeldungen chronologisch eingetragen werden, um auch zu einem späteren Zeitpunkt die Rückverfolgung von Aufträgen zu gewährleisten.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Statusprotokoll	Stand: 02.02.1998	Seite: 33

Realisierung Bank: verpflichtend
Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Statusprotokoll anfordern
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKPRO
Bezugssegment: -
Segmentversion: 2
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Maximale Anzahl Einträge	DE	num	..4	K	1	>0
3	Aufsetzpunkt	DE	an	..35	K	1	

◆ Erläuterungen

Nr. 2: Maximale Anzahl Einträge

Es kann die Anzahl der rückzumeldenden Statusprotokolleinträge begrenzt werden (s. Kap. II.7.3).

Nr. 3: Aufsetzpunkt

Belegung nur zulässig, wenn vom Kreditinstitut ein Aufsetzpunkt zurückgemeldet wurde (s. Kap. II.7.3).

◆ Beispiel

HKPRO : 3 : 2 '

b) Kreditinstitutsrückmeldung

◆ Beschreibung

Für jeden Auftrag, für den ein Statusprotokoll verfügbar ist, ist ein Segment bzw. mehrere Segmente mit nachfolgendem Format in die Antwortnachricht einzustellen.

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 34	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Statusprotokoll

◆ Format

Name: Statusprotokoll rückmelden
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIPRO
 Bezugssegment: HKPRO
 Segmentversion: 2
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Bezugsnachricht	DEG			M	1	
3	Bezugssegment	DE	num	..3	K	1	>=1
4	Datum	DE	dat	#	M	1	
5	Uhrzeit	DE	tim	#	M	1	
6	Rückmeldung	DEG			M	1	

◆ Erläuterungen

Nr. 2: Bezugsnachricht

Einzustellen ist die Referenz auf die Kundennachricht, auf die sich die Statusmeldung bezieht.

Format u. Belegung: s. Kap. II.6.2

Nr. 3: Bezugssegment

Einzustellen ist die Segmentnummer des Kundenauftrags, auf das sich die Statusmeldung bezieht. Falls sich die Statusmeldung nicht auf einen Auftrag, sondern auf die Gesamtnachricht bezieht, ist das DE nicht zu belegen.

Nr. 4: Datum

Datum der Einreichung des Auftrags

Nr. 5: Uhrzeit

Uhrzeit der Einreichung des Auftrags

Nr. 6: Rückmeldung

Format u. Belegung: s. Kap. II.8.5.2

◆ Beispiel

```

HIPRO:4:2:3+4711:3+4+19960210+113025+0020::Auftrag ausgeführt'
HIPRO:5:2:3+4711:3+5+19960210+113025+9210:3,1:Kontonummer ungültig'
  
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Statusprotokoll	Stand: 02.02.1998	Seite: 35

c) Bankparameterdaten

◆ Format

Name: Statusprotokoll Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIPROS
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Die DEG wird nicht belegt.

◆ Beispiel

HIPROS:11:2:5+1+1+2 '

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 36	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Synchronisierung

III.8 Synchronisierung

Eine Synchronisierung ist erforderlich, wenn

- für das vom Kunden verwendete Endgerät noch keine Kundensystem-ID vergeben wurde. Dies ist nur bei Verwendung des RDH-Verfahrens erforderlich, da bei symmetrischen Signatur- und Verschlüsselungsverfahren kreditinstitutsseitig keine Verwaltung respektive Generierung einer Kundensystem-ID erfolgt. Im Rahmen der Dialoginitialisierungs-Antwortnachricht erhält das entsprechende Kundensystem eine neue Kundensystem-ID mitgeteilt.
- aufgrund eines Verbindungsabbruchs nicht ersichtlich ist, welche Nachrichten vom Kreditinstitut bereits entgegengenommen wurden. In diesem Fall wird dem Kunden in der Antwort die Nummer der im vorangegangenen Dialog vom Kreditinstitut zuletzt verarbeiteten Nachricht zurückgemeldet (s. auch Kap. „Verbindungsabbruch“). Eine Synchronisierung der Nachrichtennummer ist daher nur für den letzten Auftragsdialog des sendenden Benutzers möglich. Eine abgebrochene Synchronisierungsnachricht überschreibt die letzte Nachrichtennummer nicht.



Das Kundensystem sollte die Synchronisierung von Nachrichten nicht automatisieren, da bei längeren Ausfallzeiten betroffene Aufträge evtl. bereits auf anderem Wege beim Kreditinstitut eingereicht wurden.

- bei Verwendung des RDH-Verfahrens die Signatur-ID abhanden gekommen ist (z.B. durch Festplattendefekt). Da bei fehlender Signatur-ID keine ordnungsgemäße Signatur erzeugt werden kann, ist in diesem Fall als Signatur-ID der reservierte Wert '9999999999999999' zu verwenden.⁵ In der Antwortnachricht wird die bisher höchste vom Benutzer bei diesem Kreditinstitut eingereichte Signatur-ID zurückgemeldet.⁶ Im DDV-Verfahren ist diese Option nicht zulässig.



Da die Signatur-ID multibankfähig ist, muß im Fall des Verlusts der Signatur-ID bei jedem Kreditinstitut, bei dem der Benutzer Signaturen eingereicht hat, eine Synchronisierung vorgenommen werden. Für zukünftige Signaturen ist dann der höchste aller zurückgemeldeten Werte inkrementiert um 1 zu verwenden.

Bestehende Aufträge, die noch nicht abgeschickt wurden, sind nach der Synchronisierung der Signatur-ID neu zu signieren, da ansonsten neu erfaßte Aufträge aufgrund einer Doppeleinreichung abgelehnt würden.

⁵ Der angegebene Wert darf nur für diese spezielle Nachricht verwendet werden. Der aktuelle Wert der Signatur-ID bleibt von dieser Belegung unberührt.

⁶ Es ist zu beachten, daß das Kreditinstitut nicht unbedingt die letzte, sondern immer die höchste eingereichte Signatur-ID zurückmeldet. Dies ist notwendig, weil die Aufträge nicht zwingend mit aufsteigender Signatur-ID beim Kreditinstitut eingereicht werden müssen und daher die Verwendung der aktuellen Signatur-ID u.U. zu einer Doppeleinreichung führen könnte.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Synchronisierung	Stand: 02.02.1998	Seite: 37

Falls eine Synchronisierungsnachricht gesendet wird, dürfen anschließend keine Auftragsnachrichten gesendet werden. Hierzu hat das Kundensystem nach dem Erhalt der Antwortnachricht eine Dialogendenachricht zu senden. Um Auftragsnachrichten zu schicken, muß das Kundenprodukt anschließend eine neue Dialoginitialisierung senden.

III.8.1 Kundennachricht

III.8.1.1 Nachrichtenformat

◆ Format

Name: Synchronisierungsnachricht
Typ: Nachricht
Sender: Kunde

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	M	1	s. Kap. VI.5.2
3	Identifikation	SEG	HKIDN	M	1	s. Kap. III.3.1.2
4	Verarbeitungsvorbereitung	SEG	HKVVB	M	1	s. Kap. III.3.1.3
5	Anforderung eines öffentlichen Schlüssels	SEG	HKISA	K	0-2	s. Kap. III.3.1.4
6	Synchronisierung	SEG	HKSYN	M	1	s. Kap. III.8.1.2
7	Signaturabschluß	SEG	HNSHA	M	1	s. Kap. VI.5.3
8	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

III.8.1.2 Segment: Synchronisierung

◆ Format

Name: Synchronisierung
Typ: Segment
Segmentart: Administration
Kennung: HKSYN
Bezugssegment: -
Segmentversion: 2
Sender: Kunde

Nr.	Name	Typ	For- mat	Län- ge	Sta- tus	An- zahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Synchronisierungsmodus	DE	num	1	M	1	0, 1, 2

Kapitel: III	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 38	Stand: 02.02.1998	Kapitel: Dialogspezifikation Abschnitt: Synchronisierung

♦ Erläuterungen

Nr. 2: Synchronisierungsmodus

Code	Bedeutung
0	Neue Kundensystem-ID zurückmelden
1	Letzte verarbeitete Nachrichtennummer zurückmelden
2	Signatur-ID zurückmelden

♦ Beispiel

HKSYN: 8 : 2+1 '

♦ Ausgewählte Beispiele für Rückmeldungs-codes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
9210	Kundensystem-ID wird vom Kreditinstitut nicht unterstützt
9210	Synchronisierung der Signatur-ID ist nicht zulässig

III.8.2 Kreditinstitutsnachricht

III.8.2.1 Nachrichtenformat

♦ Beschreibung

Das Kreditinstitut meldet dem Kundensystem je nach Kundenanforderung entweder die neu zugeteilte Kundensystem-ID, die zuletzt erhaltene Nachrichtennummer des vorangegangenen Dialoges oder die aktuelle Signatur-ID (Sicherheitsreferenznummer) zurück.

♦ Format

Name: Synchronisierungsantwortnachricht
Typ: Nachricht
Sender: Kreditinstitut

Nr.	Name	Typ	Ken-nung	Sta-tus	An-zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	K	1	s. Kap. VI.5.2
3	Rückmeldungen zur Gesamtnachricht	SEG	HIRMG	M	1	s. Kap. II.8.2
4	Rückmeldungen zu Segmenten	SEG	HIRMS	K	0..n	s. Kap. II.8.3
5	Bankparameterdaten	SF	#	K	1	s. Kap. III.3.2.2
6	Userparameterdaten	SF	#	K	1	s. Kap. III.3.2.3
7	Übermittlung eines öffentlichen Schlüssels	SEG	HIISA	K	0-2	s. Kap. III.3.2.4
8	Synchronisierungsantwort	SEG	HISYN	M	1	s. Kap. III.8.2.2
9	Kreditinstitutsmeldung	SEG	HIKIM	K	0..n	s. Kap. III.3.2.5
10	Signaturabschluß	SEG	HNSHA	K	1	s. Kap. VI.5.3
11	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: III
Kapitel: Dialogspezifikation Abschnitt: Synchronisierung	Stand: 02.02.1998	Seite: 39

III.8.2.2 Segment: Synchronisierungsantwort

◆ Format

Name: Synchronisierungsantwort
 Typ: Segment
 Segmentart: Administration
 Kennung: HISYN
 Bezugssegment: HKSYN
 Segmentversion: 3
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kundensystem-ID	DE	id	#	K	1	
3	Nachrichtennummer	DE	num	..4	K	1	>0
4	Sicherheitsreferenznummer	DE	num	..16	K	1	

◆ Beispiel

HISYN:10:3:8+2 '

HISYN:10:3:8++3 '

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: IV
Kapitel: Bankparameterdaten (BPD) Abschnitt: Inhaltsverzeichnis	Stand: 02.02.1998	Seite: 1

IV. BANKPARAMETERDATEN (BPD)

IV.1 Allgemeines	3
IV.2 Bankparameter allgemein	5
IV.3 Kommunikationszugang.....	7
IV.4 Sicherheitsverfahren	8
IV.5 Komprimierungsverfahren	10
IV.6 Geschäftsvorfallparameter	11
IV.7 Parameterdaten.....	13

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: IV
Kapitel: Bankparameterdaten (BPD) Abschnitt: Allgemeines	Stand: 02.02.1998	Seite: 3

IV.1 Allgemeines

◆ Beschreibung

Die Bankparameterdaten dienen zum einen der automatisierten kreditinstitutsspezifischen Konfiguration von Kundensystemen und zum anderen der dynamischen Anpassung an institutsseitige Vorgaben hinsichtlich der Auftragsgenerierung.

Des weiteren ist es mit Hilfe der BPD möglich, bestimmte Fehler bereits auf der Kundenseite zu erkennen, was sich wiederum positiv auf die institutsseitige Verarbeitung der Auftragsdaten auswirkt.

Beispiel:

Zur Einreichung einer Überweisung bei einem Kreditinstitut, das nur zwei Zeilen Verwendungszweckangaben zuläßt, hat der Kunde im entsprechenden Bildschirmformular auch nur zwei Eingabezeilen zur Verfügung. Bei der Einreichung einer Überweisung bei einem Kreditinstitut, das vier Verwendungszweckzeilen unterstützt, erscheinen vier Zeilen im Bildschirmformular.

Bei korrekter Nutzung durch das Kundensystem verhindert dieser Mechanismus somit, daß Informationen an die Kreditinstitute gesendet werden, die diese nicht darstellen bzw. verarbeiten können.



Da auf Schnittstellenebene nicht gewährleistet werden kann, daß das Kundenprodukt die Bankparameterdaten korrekt auswertet, hat auf jeden Fall eine entsprechende kreditinstitutsseitige Prüfung stattzufinden.

Bei kreditinstitutsseitigen Änderungen werden die aktualisierten Bankparameterdaten dem Kunden beim nächsten Dialog automatisch im Rahmen der Dialoginitialisierung übermittelt. Die neuen BPD werden sofort, d.h. schon für den laufenden Dialog, aktiv.



Intelligente Kundenprodukte können in diesem Fall im laufenden Dialog die Einhaltung der BPD prüfen und die Auftragsnachrichten wie geplant senden, falls die BPD-Änderungen keine Auswirkung auf die zur Versendung anstehenden Aufträge haben. Steht diese Intelligenz nicht zur Verfügung, so muß nach Erhalt der neuen BPD der laufende Dialog vom Kunden (Kundenprodukt) beendet, die Aufträge geprüft bzw. neu erfaßt und dann ein neuer Dialog begonnen werden.

In Abgrenzung zu den UPD enthalten die BPD ausschließlich Daten, die für das jeweilige Kreditinstitut spezifisch sind, und damit eher seltener geändert werden müssen.

Ist zur Belegung von DEs keine Angabe gemacht (z.B. Signaturverfahren etc.), erfolgt die Belegung wie in der entsprechenden Nachricht/Segment.

Kapitel: IV	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 4	Stand: 02.02.1998	Kapitel: Bankparameterdaten (BPD) Abschnitt: Allgemeines

Realisierung Bank: verpflichtend

Realisierung Kunde: verpflichtend



Werden Bankparameterdaten in einer Form übergeben, die eine Dateibenennung erfordert (z.B. auf Diskette), ist als Name für Bankparameterdaten "*.BPD" zu wählen, wobei "*" durch die jeweilige Kreditinstitutskenntung (Bankleitzahl) zu ersetzen ist.

Über die Angebote fremder Kreditinstitute kann sich der Kunde mit Hilfe derer BPD informieren. Es wird empfohlen, Kundenprodukte standardmäßig mit einer Auswahl von Bankparameterdaten gängiger Kreditinstitute auszustatten. Falls diese nicht auf dem Kundensystem verfügbar sind, muß ein Dialog mit dem Fremdinstitut geführt werden, während dessen die aktuellen BPD automatisch übertragen werden. Zur erstmaligen Verbindungsaufnahme mit dem Fremdinstitut sind dessen Zugangsdaten erforderlich. Diese erhält das Kundenprodukt entweder durch den Abruf der Kommunikationszugangsdaten (s. Kap. VIII.7) oder auf anderem Wege (z.B. direkt von seinem Institut). Im letzteren Fall müssen die Zugangsdaten manuell eingegeben werden.

◆ Format

Name: Bankparameterdaten
Typ: Segmentfolge
Sender: Kreditinstitut

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Bankparameter allgemein	SEG	HIBPA	M	1	s. Kap. IV.2
2	Kommunikationszugang rückmelden	SEG	HIKOM	K	0..1	s. Kap. IV.3
3	Sicherheitsverfahren	SEG	HISHV	K	0..1	s. Kap. IV.4
4	Komprimierungsverfahren	SEG	HIKPV	K	0..1	s. Kap. IV.5
5	Parameterdaten	SF	#	K	1	s. Kap. IV.7

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: IV
Kapitel: Bankparameterdaten (BPD) Abschnitt: Bankparameter allgemein	Stand: 02.02.1998	Seite: 5

IV.2 Bankparameter allgemein

◆ Format

Name: Bankparameter allgemein
 Typ: Segment
 Segmentart: Administration
 Kennung: HIBPA
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	BPD-Version	DE	num	..3	M	1	
3	Kreditinstitutskennung	DEG	kik	#	M	1	
4	Kreditinstitutsbezeichnung	DE	an	..60	M	1	
5	Anzahl Geschäftsvorfällearten	DE	num	..3	M	1	1
6	Unterstützte Sprachen	DEG			M	1	
7	Unterstützte HBCI-Versionen	DEG			M	1	
8	Maximale Nachrichten-größe	DE	num	..4	K	1	

◆ Erläuterungen

Nr. 2: BPD-Version

Hierbei handelt es sich um eine kreditinstitutsseitig vergebene Versionsnummer der BPD, die den jeweiligen Stand der institutsspezifischen Unterstützung des Homebankings kennzeichnet (bei jeder für das Kundensystem relevanten Änderung des Kreditinstitutssystems werden neue BPD mit einer neuen BPD-Versionsnummer kreditinstitutsseitig bereitgestellt). Diese BPD-Versionsnummer ist unabhängig von der Version des BPD-Nachrichtenformats, die im Nachrichtenkopf eingestellt ist und lediglich das Format der Nachricht, nicht jedoch deren Inhalt kennzeichnet.

Nr. 3: Kreditinstitutskennung

Es ist die Institutskennung des Kreditinstituts einzustellen, auf das sich die nachfolgenden Bankparameterdaten beziehen.

Nr. 4: Kreditinstitutsbezeichnung

Es ist die Bezeichnung des Instituts einzustellen. Diese ist vom Kreditinstitut frei wählbar.

Nr. 5: Anzahl Geschäftsvorfällearten

Hier kann das Kreditinstitut die maximale Anzahl an Geschäftsvorfällearten einstellen, die pro Nachricht zulässig ist. In der aktuellen HBCI-Version ist lediglich eine Geschäftsvorfälleart pro Nachricht erlaubt (z.B. nur HKUEB).

Falls keine Restriktionen bzgl. der Anzahl an Geschäftsvorfällearten bestehen, ist der Wert 0 einzustellen.

Kapitel: IV	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 6	Stand: 02.02.1998	Kapitel: Bankparameterdaten (BPD) Abschnitt: Bankparameter allgemein

Nr. 6: Unterstützte Sprachen

Hier stellt das Kreditinstitut ein, in welcher Sprache der Kunde mit dem Kreditinstitut kommunizieren kann. Die derzeit gültigen Sprachkennzeichen sind im Kap. „Dialoginitialisierung“ im Segment „Verarbeitungsvorbereitung“ aufgeführt.

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Unterstützte Sprache	GD	num	..3	M	1..9	1, 2, 3



Bei Bedarf kann das Kundenprodukt auf dieses Kennzeichen reagieren und die Sprache des Kundenproduktes entsprechend automatisiert anpassen.

Nr. 7: Unterstützte HBCI-Versionen

Es ist diejenige HBCI-Version einzustellen, die das Kreditinstitut für den Aufbau der Nachrichten zugrunde legt.

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Unterstützte HBCI-Version	GD	num	..3	M	1..9	

Nr. 8: Maximale Nachrichtengröße

Sofern im Kreditinstitut technische Restriktionen bzgl. der Verarbeitung umfangreicher Kundennachrichten bestehen, kann das Kreditinstitut eine Obergrenze in Kilobyte (=1024 Byte) einstellen. Eingehende Nachrichten, die dekomprimiert und entschlüsselt diese Grenze überschreiten, können abgelehnt werden.

Falls keine Restriktionen bzgl. der Nachrichtengröße bestehen, ist der Wert 0 einzustellen.



Sollte dieses DE belegt sein, hat das Kundenprodukt bei der Zusammenstellung der Nachricht diese Restriktion zu beachten. Zu große Nachrichten dürfen nicht zur Versendung freigegeben werden. Eventuell hat das Kundenprodukt Nachrichten, die aus mehreren Aufträgen bestehen, in mehrere kleinere Nachrichten mit je einem Auftrag aufzuteilen. Kann die Nachrichtengröße bei umfangreichen Einzelaufträgen (z.B. Sammelüberweisungen) nicht verringert werden, so ist der Auftrag anwendungsseitig zu verkleinern.

◆ Beispiel

```
HIBPA:3:2:7+3+280:10020030+Musterbank in Musters  
tadt+1+1:2:3+1+100'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: IV
Kapitel: Bankparameterdaten (BPD) Abschnitt: Kommunikationszugang	Stand: 02.02.1998	Seite: 7

IV.3 Kommunikationszugang

◆ Beschreibung

Dieses Segment enthält transportmedienspezifische Informationen, die für den Zugang zum Kreditinstitut erforderlich sind.



Für den Erstzugang oder den anonymen Zugang ist die Einstellung dieser Informationen in den BPD nicht hilfreich, da in diesem Fall zum Zeitpunkt des Zugangs die entsprechenden BPD noch nicht vorliegen. Die vom Kundenprodukt benötigten Zugangsinformationen sollten daher durch den Abruf der Kommunikationszugangsdaten (s. Kap. VIII.7) angefordert werden.

Die Einstellung dieser Daten erfolgt dennoch redundant in den BPD, um einerseits dem Kundenprodukt Änderungen der Zugangsparameter ohne Aktualisierung der Zugangsdatenbank mitzuteilen und andererseits den Zugang auch ohne Zugangsdatenbank zu ermöglichen, sofern das Kundenprodukt die BPD bereits vorliegen hat (bspw. auf Diskette).



Grundsätzlich gelten für alle Kommunikationszugänge eines Instituts dieselben Bankparameterdaten (BPD). Möchte das Kreditinstitut seine Angebote (z.B. die erlaubten Geschäftsvorfälle) abhängig vom Kommunikationsmedium gestalten, so besteht die Möglichkeit, für bestimmte Kommunikationszugänge eine eigene, noch nicht belegte BLZ zu vergeben.

◆ Format

Name: Kommunikationszugang [rückmelden](#)
Typ: Segment
Segmentart: Administration
Kennung: HIKOM
Bezugssegment: HKVVB
Segmentversion: s. Kap. VIII.7
Sender: Kreditinstitut
Format: s. Kap. VIII.7

Kapitel: IV	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 8	Stand: 02.02.1998	Kapitel: Bankparameterdaten (BPD) Abschnitt: Sicherheitsverfahren

IV.4 Sicherheitsverfahren

◆ Beschreibung

Es sind die Sicherheitsverfahren, d.h. Signatur- und Verschlüsselungsalgorithmen, anzugeben, die das Kreditinstitut unterstützt.

◆ Format

Name: Sicherheitsverfahren
 Typ: Segment
 Segmentart: Administration
 Kennung: HISHV
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Mischung zulässig	DE	jn	#	M	1	
3	Unterstützte Sicherheitsverfahren	DEG			M	1..9	

◆ Erläuterungen

Nr. 2: Mischung zulässig

Es ist anzugeben, ob das Kreditinstitut die Mischung von Sicherheitsverfahren zulässt, sofern es mehrere Sicherheitsverfahren anbietet. Hierunter ist zu verstehen,

- daß eine Nachricht von mehreren Benutzern mit unterschiedlichen Verfahren signiert wird.
- daß ein Benutzer die Nachrichten eines Dialoges mit verschiedenen Verfahren signiert.
- daß Signatur und Verschlüsselung einer Nachricht mit verschiedenen Verfahren durchgeführt werden.

Ist hier 'N' eingestellt, so sind die genannten Fälle nicht zulässig, d.h. alle Signaturen und Verschlüsselungen eines Dialoges müssen mit demselben Sicherheitsverfahren vorgenommen werden. Ist 'J' eingestellt, so müssen kreditinstitutsseitig alle vorgenannten Fälle unterstützt werden.

Falls das Kreditinstitut nur ein Sicherheitsverfahren anbietet, ist 'N' einzustellen.

Nr. 3: Unterstützte Sicherheitsverfahren

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Sicherheitsverfahren, Code	GD	an	3	M	1	DDV, RDH
2	Version des Sicherheitsverfahrens	GD	num	..3	M	1..9	

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: IV
Kapitel: Bankparameterdaten (BPD) Abschnitt: Sicherheitsverfahren	Stand: 02.02.1998	Seite: 9

Nr. 1: Sicherheitsverfahren, Code

Es ist der Code des unterstützten Signatur- bzw. Verschlüsselungsalgorithmus einzustellen.

Code	Bedeutung
DDV	DES-DES-Verfahren
RDH	RSA-DES-Hybridverfahren

Weitere Informationen zu den Verfahren sind dem Kapitel VI.1 zu entnehmen.

Nr. 2: Version des Sicherheitsverfahrens

Es sind die Versionen des unterstützten Sicherheitsalgorithmus einzustellen.

◆ Beispiel

HISHV: 5: 2: 7+N+RDH: 3: 2: 1 '

Kapitel: IV	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 10	Stand: 02.02.1998	Kapitel: Bankparameterdaten (BPD) Abschnitt: Komprimierungsverfahren

IV.5 Komprimierungsverfahren

◆ Beschreibung

Dieses Segment darf z.Zt. nicht gesendet werden, da in der vorliegenden Version keine Komprimierung zulässig ist. Dennoch findet an dieser Stelle eine Spezifikation des benötigten Segmentformates statt, damit zu einem späteren Zeitpunkt diese Funktionalität mit geringem Aufwand hinzugefügt werden kann.

◆ Format

Name: Komprimierungsverfahren
 Typ: Segment
 Segmentart: Administration
 Kennung: HIKPV
 Bezugssegment: HKVVB
 Segmentversion: 1
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Unterstützte Komprimierungsverfahren	DEG			M	1..9	

◆ Erläuterungen

Nr. 2: Unterstützte Komprimierungsverfahren

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Komprimierungsfunktion	GD	an	..3	M	1	0
2	Komprimierungsversion	GD	num	..3	M	1..9	0

Nr. 1: Komprimierungsfunktion

Es ist der Code der unterstützten Komprimierungsfunktion einzustellen. Die derzeit gültigen Verfahren sind dem Kapitel VI.5.4 zu entnehmen.

Nr. 2: Komprimierungsversion

Es sind die Versionen der unterstützten Komprimierungsfunktion einzustellen.

◆ Beispiel

HIKPV:6:1:7+0:0'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: IV
Kapitel: Bankparameterdaten (BPD) Abschnitt: Geschäftsvorfallparameter	Stand: 02.02.1998	Seite: 11

IV.6 Geschäftsvorfallparameter

◆ Beschreibung

Dieses Segment beschreibt anhand von Parametern die konkrete kreditinstitutsindividuelle Ausgestaltung eines Geschäftsvorfalles.

Das Segment ist für jeden Geschäftsvorfall einzustellen, den das Kreditinstitut unterstützt. Geschäftsvorfälle sind hierbei alle Auftragssegmente mit der Segmentart „Geschäftsvorfall“. Bei Nichtunterstützung eines Geschäftsvorfalles entfällt das Segment. Falls mehrere Versionen des Geschäftsvorfalles unterstützt werden, ist das Segment für jede Segmentversion einzustellen. Die Zuordnung der Geschäftsvorfallparameter zur jeweiligen Version des Geschäftsvorfalles erfolgt hierbei durch die im Segmentkopf angegebene Segmentversion (s. Kap. II.6.1).



Es ist dem Kreditinstitut freigestellt, ob es in den Bankparameterdaten grundsätzlich alle Segmentversionen eines Geschäftsvorfalles einstellt, die es unterstützt oder nur diejenigen, die in Abhängigkeit von der HBCI-Version, die der Kunde in der Dialoginitialisierung mitteilt, im aktuellen Dialog als gültig entgegengenommen würden.

◆ Format

Name: Geschäftsvorfallparameter
Typ: Format

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Maximale Anzahl Aufträge	DE	num	..3	M	1	
3	Anzahl Signaturen mindestens	DE	num	1	M	1	0, 1, 2, 3
4	Parameter	DEG			K	1	

◆ Erläuterungen

Nr. 2: Maximale Anzahl Aufträge

Höchstens zulässige Anzahl an Segmenten des jeweiligen Auftragsart je Kundennachricht. Übersteigt die Anzahl der vom Kunden übermittelten Segmente pro Auftragsart die zugelassene Maximalanzahl, so wird die gesamte Nachricht abgelehnt.

Nr. 3: Anzahl Signaturen **mindestens**

Es wird immer die Minimalanforderung an einen Geschäftsvorfall mitgeteilt, d.h. '0', wenn der Geschäftsvorfall auch über den anonymen Zugang angeboten wird, ansonsten mindestens '1', da Aufträge von Kunden immer signiert werden müssen.

Die für Kunden jeweils genaue Angabe der Signaturanzahl ergibt sich in den UPD aus dem Feld „Anzahl benötigter Signaturen“. Dabei muß die in

Kapitel: IV	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 12	Stand: 02.02.1998	Kapitel: Bankparameterdaten (BPD) Abschnitt: Geschäftsvorfallparameter

den UPD angegebene Signaturanzahl größer oder gleich der in den BPD angegebene Anzahl sein. Für Institute, die keine UPD unterstützen, bedeutet dies, daß der Eintrag '0' in den BPD nur für Nichtkunden gilt und für Kunden als 'mindestens 1' zu interpretieren ist.

Wert gilt für alle Signaturverfahren.

Nr. 4: Parameter

Gestaltungsmöglichkeiten des Geschäftsvorfalls, beispielsweise Anzahl der erlaubten Verwendungszweckzeilen bei Überweisungen. Diese DEG hat je nach beschriebener Segmentart einen unterschiedlichen Aufbau.

Der jeweilige Aufbau wird beim zugehörigen Geschäftsvorfall beschrieben.

◆ Beispiel

HIUEBS:6:2:5+1+2+14:51:53:54:67:69 '

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: IV
Kapitel: Bankparameterdaten (BPD) Abschnitt: Parameterdaten	Stand: 02.02.1998	Seite: 13

IV.7 Parameterdaten

◆ Beschreibung

Die Segmentfolge „Parameterdaten“ enthält die im Kapitel „Geschäftsvorfallparameter“ beschriebenen Parametersegmente.

◆ Format

Name: Parameterdaten
Typ: Segmentfolge
Sender: Kreditinstitut

◆ Erläuterungen

Die Reihenfolge der Segmente ist nicht erheblich.

◆ Beispiel

```
HIUEBS:6:1:5+1+2+7:51:53:54:67:69'
HIUEBS:7:2:5+1+2+14:51:53:54:67:69'
HIKAZS:8:4:5+1+2+60:J'
HISALS:9:3:5+1+2'
```


Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: V
Kapitel: Userparameterdaten (UPD) Abschnitt: Inhaltsverzeichnis	Stand: 02.02.1998	Seite: 1

V. USERPARAMETERDATEN (UPD)

V.1 Allgemeines	3
V.2 Userparameter allgemein	4
V.3 Kontoinformation	5

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: V
Kapitel: Userparameterdaten (UPD) Abschnitt: Allgemeines	Stand: 02.02.1998	Seite: 3

V.1 Allgemeines

◆ Beschreibung

Die Userparameterdaten, die kreditinstitutsseitig benutzerbezogen generiert und vorgehalten werden, erlauben eine automatisierte und dynamische Konfiguration von Kundensystemen. In Abgrenzung zu den BPD enthalten die UPD ausschließlich kunden- und kontenspezifische Informationen und sind somit häufigeren Modifikationen unterworfen.

Bei Änderungen werden die Userparameterdaten im Rahmen der Dialoginitialisierung für den sich anmeldenden Benutzer automatisch aktualisiert. Die aktualisierten UPD werden sofort aktiv (s. hierzu die Ausführungen zu den BPD).

Realisierung Bank: verpflichtend

Realisierung Kunde: verpflichtend



Da auf Schnittstellenebene nicht gewährleistet werden kann, daß das Kundenprodukt die Userparameterdaten korrekt auswertet, hat auf jeden Fall eine entsprechende kreditinstitutsseitige Prüfung stattzufinden.



(s. auch Hinweise bei „Bankparameterdaten“)

Die Nutzung der UPD erfordert eine entsprechende Unterstützung durch das Kundenprodukt. Dateiname (sofern erforderlich) ist "*.upd", wobei "*" durch eine eindeutige Kennung, die den Benutzer angibt, zu ersetzen ist.

◆ Format

Name: Userparameterdaten

Typ: Segmentfolge

Sender: Kreditinstitut

Nr.	Name	Typ	Kennung	Status	Anzahl	Anmerkungen
1	Userparameter allgemein	SEG	HIUPA	M	1	
2	Kontoinformation	SEG	HIUPD	K	0..n	

Kapitel:	V	Version:	2.0.1	Homebanking-Computer-Interface (HBCI)
Seite:	4	Stand:	02.02.1998	Kapitel: Userparameterdaten (UPD) Abschnitt: Userparameter allgemein

V.2 Userparameter allgemein

◆ Format

Name: Userparameter allgemein
 Typ: Segment
 Segmentart: Administration
 Kennung: HIUPA
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Benutzerkennung	DE	id	#	M	1	
3	UPD-Version	DE	num	..3	M	1	
4	UPD-Verwendung	DE	num	1	M	1	0, 1

◆ Erläuterungen

Nr. 2: Benutzerkennung

Es ist die Benutzerkennung des Benutzers anzugeben, auf den sich die Userparameterdaten beziehen (s. Kap. III.1.1).

Nr. 3: UPD-Version

Versionsnummer der UPD. Bei jeder kreditinstitutsseitigen Änderung wird die Version inkrementiert.

s. auch DE „BPD-Version“ (Kap. IV.2)

Nr. 4: UPD-Verwendung

Dieses Kennzeichen gibt an, wie diejenigen Geschäftsvorfälle zu interpretieren sind, die bei der Beschreibung der Kontoinformationen nicht unter den erlaubten Geschäftsvorfällen aufgeführt sind:

Status	Beschreibung
0	Die nicht aufgeführten Geschäftsvorfälle sind gesperrt (die aufgeführten Geschäftsvorfälle sind zugelassen).
1	Bei den nicht aufgeführten Geschäftsvorfällen ist anhand der UPD keine Aussage darüber möglich, ob diese erlaubt oder gesperrt sind. Diese Prüfung kann nur online vom Kreditinstitutssystem vorgenommen werden.

Bsp.: Im Beispiel unter Kap. V.3 ist im ersten Fall (Status=0) die Sammelüberweisung (HKSUB) gesperrt. Im zweiten Fall ist sie entweder erlaubt oder gesperrt.

◆ Beispiel

HIUPA:14:1:7+12345+4+0 '

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: V
Kapitel: Userparameterdaten (UPD) Abschnitt: Kontoinformation	Stand: 02.02.1998	Seite: 5

V.3 Kontoinformation

◆ Beschreibung

Das Segment „Kontoinformation“ ist für jedes Konto, für das der Benutzer beim betreffenden Kreditinstitut eine Verfügungsberechtigung besitzt, einzustellen.

◆ Format

Name: Kontoinformation
 Typ: Segment
 Segmentart: Administration
 Kennung: HIUPD
 Bezugssegment: HKVVB
 Segmentversion: 3
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kontoverbindung	DEG	kto	#	M	1	
3	Kunden-ID	DE	id	#	M	1	
4	Kontowährung	DE	cur	#	K	1	
5	Name 1	DE	an	..27	M	1	
6	Name 2	DE	an	..27	K	1	
7	Kontoproduktbezeichnung	DE	an	..30	K	1	
8	Kontolimit	DEG			K	1	
9	Erlaubte Geschäftsvorfälle	DEG			K	999	

◆ Erläuterungen

Nr. 2: Kontoverbindung

Es ist die Kontoverbindung des Kunden einzustellen, auf die sich nachfolgende Informationen beziehen.

Nr. 3: Kunden-ID

Rolle, die dem Benutzer für diese Konto zugeordnet wurde (s. Kap. III.1.1).

Nr. 4: Kontowährung

ISO-Währungscode der Währung, in der das Konto geführt wird. Bei Depotkonten kann auf die Angabe der Kontowährung verzichtet werden.

Nr. 5,6: Name 1, Name 2

Zu Informationszwecken wird der Name des Kontoinhabers eingestellt.

Nr. 7: Kontoproduktbezeichnung

Es kann eine Produktbezeichnung des Kontos eingestellt werden. Die Bezeichnung ist vom Kreditinstitut frei wählbar.

Nr. 8: Kontolimit

Die Angabe eines Kontolimits ist kreditinstitutsseitig optional. Daher kann für den Kunden ein Limit bestehen, auch wenn dieses nicht in die UPD ein-

Kapitel: V	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 6	Stand: 02.02.1998	Kapitel: Userparameterdaten (UPD) Abschnitt: Kontoinformation

gestellt wurde. Ein kontobezogenes Limit darf nicht gleichzeitig mit geschäftsvorfallbezogenen Limiten angegeben werden.

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Limitart	GD	an	1	M	1	E, T, W, M, Z
2	Limitbetrag	GDG	btg	#	M	1	
3	Limit-Tage	GD	num	..3	K	1	>0

Erläuterungen s.u.

Nr. 9: Erlaubte Geschäftsvorfälle

Der Benutzer erhält die Information, ob er zur Ausführung des jeweiligen Geschäftsvorfalles zugelassen ist und wie viele Signaturen hierzu mindestens erforderlich sind. Ferner können für jeden Geschäftsvorfall Einzelauftragslimite angegeben werden, sofern dies bankfachlich möglich ist. Die Reihenfolge der Geschäftsvorfälle ist unerheblich.

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Geschäftsvorfall	GD	an	..6	M	1	
2	Anzahl benötigter Signaturen	GD	num	..2	M	1	0, 1, 2, 3
3	Limitart	GD	an	1	K	1	E, T, W, M, Z
4	Limitbetrag	GDG	btg	#	K	1	
5	Limit-Tage	GD	num	..3	K	1	>0

Nr. 1: Geschäftsvorfall

Es sind die Geschäftsvorfälle anzugeben, für deren Ausführung der Benutzer berechtigt ist. Hierzu gehören neben den Auftragssegmenten mit der Segmentart „Geschäftsvorfall“ auch die Segmente der Key-Management-Nachrichten. Einzustellen ist jeweils die Segmentkennung des Kundensegments.

Nr. 2: Anzahl benötigter Signaturen

Falls 0 angegeben ist, handelt es sich um einen nicht signierungspflichtigen Geschäftsvorfall, der auch über einen anonymen Zugang ohne Signierungsmöglichkeit ausgeführt werden kann.

Falls die Anzahl der benötigten Signaturen größer als 1 ist, bedeutet dies, daß dieser Geschäftsvorfall zusätzlich von mindestens einem anderen berechtigten Benutzer signiert werden muß, über dessen Identität in den UPD jedoch nichts ausgesagt wird.

Nr. 3: Limitart

Es kann ein geschäftsvorfallbezogenes Limit eingestellt werden. Dies ist jedoch nur möglich, wenn nicht gleichzeitig ein kontobezogenes Limit angegeben wurde. Die Angabe eines Limits ist kreditinstitutsseitig optional. Daher kann für den Kunden ein Limit bestehen, auch wenn dieses nicht in die UPD eingestellt wurde.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: V
Kapitel: Userparameterdaten (UPD) Abschnitt: Kontoinformation	Stand: 02.02.1998	Seite: 7

Code	Beschreibung
E	Einzelauftragslimit
T	Tageslimit
W	Wochenlimit
M	Monatslimit
Z	Zeitlimit

Nr. 4: Limitbetrag

Betrag für Userlimit.

Nr. 5: Limit-Tage

Anzahl Tage für rollierendes Zeitlimit (Limitart 'Z'). Belegung ist nur bei Zeitlimit zulässig.

◆ Beispiel

```
HIUPD:15:3:7+1234567:280:10020030+12345+DEM+Ernst
Müller++Giro Spezial+T:2000,:DEM+HKPRO:1+HKSAK
:1+HKISA:1+HKSSP:1+HKUEB:1+HKLAS:1+HKKAN:1+HKKAZ
:1+HKSAL:1'
```

```
HIUPD:16:3:7+1234568:280:10020030+12345+DEM+Ernst
Müller++Sparkonto 2000++HKPRO:1+HKSAK:0+HKISA:
1+HKSSP:0+HKUEB:2:Z:1000,:DEM:7+HKKAN:1+HKKAZ:1+
HKSAL:2'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Inhaltsverzeichnis	Stand: 02.02.1998	Seite: 1

VI. SICHERHEIT

VI.1 Allgemeines	3
VI.2 Mechanismen	4
VI.2.1 Elektronische Signatur	4
VI.2.1.1 Elektronische Signatur bei DDV (DES-basierend)	4
VI.2.1.2 Elektronische Signatur bei RDH (RSA-basierend)	5
VI.2.2 Verschlüsselung.....	5
VI.2.2.1 Verschlüsselung bei DDV (DES-basierend)	8
VI.2.2.2 Verschlüsselung bei RDH (RSA-basierend)	9
VI.2.3 Sicherheitsmedien beim Kundenprodukt	10
VI.3 Abläufe.....	11
VI.3.1 Schlüsselverwaltung	11
VI.3.1.1 Gemeinsam verwendete Verfahren zur Schlüsselverwaltung.....	11
VI.3.1.2 Symmetrische Schlüssel für DDV	12
VI.3.1.2.1 Schlüsselgenerierung.....	12
VI.3.1.2.2 Initiale Schlüsselverteilung	13
VI.3.1.2.3 Schlüsseländerungen.....	13
VI.3.1.2.4 Schlüsselverteilung nach Kompromittierung	13
VI.3.1.3 Asymmetrische Schlüssel für RDH	14
VI.3.1.3.1 Schlüsselgenerierung.....	14
VI.3.1.3.2 Initiale Schlüsselverteilung	15
VI.3.1.3.3 Schlüsseländerungen.....	19
VI.3.1.3.4 Schlüsselverteilung nach Kompromittierung	19
VI.3.2 Doppeleinreichungskontrolle.....	20
VI.3.3 Schlüsselsperrung	20
VI.4 Bankfachliche Anforderungen	22
VI.5 Formate für Signatur und Verschlüsselung	23
VI.5.1 Mehrfach verwendete Datenelementgruppen	24
VI.5.1.1 Schlüsselname	24
VI.5.1.2 Sicherheits-/Gültigkeitsdatum und -uhrzeit	26
VI.5.1.3 Sicherheitsidentifikation, Details	27
VI.5.1.4 Zertifikat.....	28
VI.5.1.5 Öffentlicher Schlüssel.....	29
VI.5.2 Signaturkopf.....	31
VI.5.2.1 Segmentbeschreibung.....	31
VI.5.2.2 Hashalgorithmus.....	34
VI.5.2.3 Signaturalgorithmus.....	35
VI.5.3 Signaturabschluß	36
VI.5.4 Verschlüsselungskopf	37
VI.5.4.1 Segmentbeschreibung.....	37
VI.5.4.2 Verschlüsselungsalgorithmus	40

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 2	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Inhaltsverzeichnis

VI.5.5 Verschlüsselte Daten	42
-----------------------------------	----

VI.6 Key-Management 43

VI.6.1 Formate für Key-Management	43
VI.6.1.1 Änderung eines öffentlichen Schlüssels	43
VI.6.1.2 Anforderung eines öffentlichen Schlüssels	45
VI.6.1.3 Übermittlung eines öffentlichen Schlüssels	47
VI.6.1.4 Schlüsselsperrung	49
VI.6.1.5 Bestätigung der Schlüsselsperrung	51
VI.6.2 Key-Management-Nachrichten	53
VI.6.2.1 Änderung eines öffentlichen Schlüssels des Kunden	53
VI.6.2.2 Erstmalige Anforderung der Schlüssel des Kreditinstituts	55
VI.6.2.3 Erstmalige Übermittlung der Schlüssel des Kunden	57
VI.6.2.4 Schlüsselsperrung durch den Kunden	60

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Allgemeines	Stand: 02.02.1998	Seite: 3

VI.1 Allgemeines

Im Rahmen von HBCI werden zeitgemäße Sicherheitsmechanismen und -methoden eingesetzt, welche den Mißbrauch der im Bereich des Homebanking eingesetzten Systeme verhindern.

Das folgende Kapitel ist in fünf Abschnitte gegliedert, welche sich mit den verwendeten Sicherheitsmechanismen, den Abläufen, den bankfachlichen Anforderungen sowie den Segmentformaten für Signatur, Verschlüsselung und Key-Management beschäftigen.

Die Ausführungen lehnen sich an bestehende deutsche Kreditinstitutsstandards (ZKA-Abkommen, z.B. DFÜ-Abkommen, ec-Chipkarte), sowie an internationale Standards (z.B. ISO, UN/EDIFACT) an.

Grundsätzlich kommen im Rahmen von HBCI zwei verschiedene Sicherheitslösungen zum Einsatz:

- eine auf dem symmetrischen DES-Verfahren basierende Chipkartenlösung
- eine auf dem asymmetrischen RSA-Verfahren basierende Lösung

Die beiden Varianten werden mit DDV (DES-DES-Verfahren), respektive RDH (RSA-DES-Hybridverfahren) gekennzeichnet. DDV verwendet den MAC als Signatur und verschlüsselt den Nachrichtenschlüssel (nachrichtenbezogener Chiffrierschlüssel) mittels 2-Key-Triple-DES, während RDH mit RSA-EU signiert und den Nachrichtenschlüssel mittels RSA chiffriert.

Angestrebt wird im Sicherheitsbereich einheitlich eine RSA-Chipkartenlösung auf Basis der derzeitigen RDH-Spezifikationen. Da diese Sicherheitskonzeption momentan aufgrund technischer Restriktionen noch nicht flächendeckend umzusetzen ist, kommt bis zur durchgehenden Realisierbarkeit der RSA-Chipkartenlösung sowohl die DDV-Lösung auf Chipkartenbasis als auch die RDH-Lösung auf reiner Softwarebasis zum Einsatz.

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 4	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Mechanismen

VI.2 Mechanismen

VI.2.1 Elektronische Signatur

Die Bildung der elektronischen Signatur erfolgt durch die Vorgänge

- Bildung des Hashwerts
- Ergänzen des Hashwerts auf eine vorgegebene Länge und
- Berechnung der elektronischen Signatur über den Hashwert.

Das Hashing ist in den beiden Verfahren DDV und RDH identisch. Die beiden anderen Verarbeitungsschritte sind jeweils verschieden.

VI.2.1.1 Elektronische Signatur bei DDV (DES-basierend)

Realisierung Bank: optional (empfohlen)

Realisierung Kunde: optional

1. Hashing der Nachricht

Als Hash-Funktion wird der RIPEMD-160 eingesetzt. Als Initialisierungsvektor dient die binäre Zeichenfolge X'67 45 23 01 EF CD AB 89 98 BA DC FE 10 32 54 76 C3 D2 E1 F0'. Der erzeugte Hashwert hat eine Länge von 20 Byte (=160 bit). (Das Padding der Nachricht auf die entsprechende Blockgröße ist im Hashverfahren implizit enthalten).

2. Formatierung des Hashwerts

Das Padding erfolgt entsprechend der folgenden Abbildung mit X'00' auf das nächste Vielfache von 8 Byte:

	Padding									
Byteposition:	24			21		20		...		1
	00	00	00	00				H a s h w e r t		

3. Berechnung der elektronischen Signatur

Als Signatur wird ein Retail CBC-MAC gemäß ANSI X9.19 gebildet. Hierzu wird der gepaddete Hashwert zunächst in 3 Blöcke der Länge 8 Byte aufgeteilt. Als Zwischenresultat wird ein einfacher CBC-MAC über die ersten 2 Blöcke berechnet. Als Initialisierungsvektor kommt X'00 00 00 00 00 00 00 00' zum Einsatz. Dabei verwendet man als Schlüssel die linke Hälfte des Signierschlüssels. Anschließend erfolgt eine 2-Key-Triple-DES-Verschlüsselung mit dem Signierschlüssel des Kunden (muß beim Kreditinstitut hergeleitet werden) über die XOR-Summe des Zwischenergebnisses mit dem letzten Nachrichtenblock. Der so erhaltene 8 Byte(=64 bit)-Ausgabeblock ist der Retail CBC-MAC.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Mechanismen	Stand: 02.02.1998	Seite: 5

VI.2.1.2 Elektronische Signatur bei RDH (RSA-basierend)

Realisierung Bank: verpflichtend

Realisierung Kunde: verpflichtend. Ausgenommen hiervon sind Endgeräte, die eine RSA-EU-Lösung noch nicht erlauben (z.B. Smartphones mit MAC-Chipkarte erlauben ggf. keine RSA-EU, PC-basierte Produkte müssen hingegen stets die RSA-EU unterstützen).

1. Hashing der Nachricht

siehe „Elektronische Signatur bei DDV“

2. **Formatierung** des Hashwerts

Die **Formatierung** erfolgt gemäß ISO 9796 (Kap. 5.1-5.4). **Der Hashwert wird für die nachfolgende Signaturbildung als Langzahl¹ interpretiert (s. auch die Beispiele in der Anlage zu ISO 9796).**

3. Berechnung der elektronischen Signatur

Der Hash-Wert wird mittels RSA signiert.

VI.2.2 Verschlüsselung

Bei der Verschlüsselung wird für jede Nachricht ein separater Nachrichtenschlüssel verwendet. Die Verschlüsselung der HBCI-Nutzdaten erfolgt generell mittels 2-Key-Triple-DES gemäß ANSI X3.92. Der Nachrichtenschlüssel wird entweder mittels 2-Key-Triple-DES (DDV) oder RSA (RDH) chiffriert und mit der verschlüsselten Nachricht mitgeliefert.



Der Nachrichtenschlüssel muß für jede Nachricht eines Dialoges individuell verschieden sein. Dies **muß** gewährleistet werden, indem das sendende System den Nachrichtenschlüssel dynamisch generiert.

Die ersten zwei Schritte sind für beide Verfahren identisch:

1. Der Sender erzeugt eine Zufallszahl als Nachrichtenschlüssel und stellt ungerade Parität sicher. Bei der Auswahl der Zufallszahl ist darauf zu achten, daß keiner der folgenden schwachen oder halbschwachen Schlüssel² gewählt wird (vgl. Kapitel VI.3.1.1).

Die schwachen Schlüssel des DES-Algorithmus:

```
X'01 01 01 01 01 01 01 01'
X'FE FE FE FE FE FE FE FE'
X'1F 1F 1F 1F 0E 0E 0E 0E'
X'E0 E0 E0 E0 F1 F1 F1 F1'
```

¹ Unter Langzahl wird dabei die kanonische Darstellung einer natürlichen Zahl in einem Feld [0..n] bezeichnet, wobei die Wertigkeit der Felder von 0 bis n abnimmt.

² Die schwachen und halbschwachen Schlüssel entsprechen denen des DFÜ-Abkommens.

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 6	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Mechanismen

Die halbschwachen Schlüssel des DES-Algorithmus:

```

X'01 FE 01 FE 01 FE 01 FE'
X'FE 01 FE 01 FE 01 FE 01'
X'1F E0 1F E0 0E F1 0E F1'
X'E0 1F E0 1F F1 0E F1 0E'
X'01 E0 01 E0 01 F1 01 F1'
X'E0 01 E0 01 F1 01 F1 01'
X'1F FE 1F FE 0E FE 0E FE'
X'FE 1F FE 1F FE 0E FE 0E'
X'01 1F 01 1F 01 0E 01 0E'
X'1F 01 1F 01 0E 01 0E 01'
X'E0 FE E0 FE F1 FE F1 FE'
X'FE E0 FE E0 FE F1 FE F1'

```

- Dieser Nachrichtenschlüssel wird verwendet, um die Daten mittels 2-Key-Triple-DES im CBC Modus gemäß ISO 10116 (ANSI X3.106) zu verschlüsseln (vgl. Abb. 13). Das Padding der Nachricht erfolgt oktettorientiert gemäß ISO 10126 (ANSI X9.23), der Initialisierungsvektor ist X'00 00 00 00 00 00 00 00' (vgl. Abb. 14 und 15).

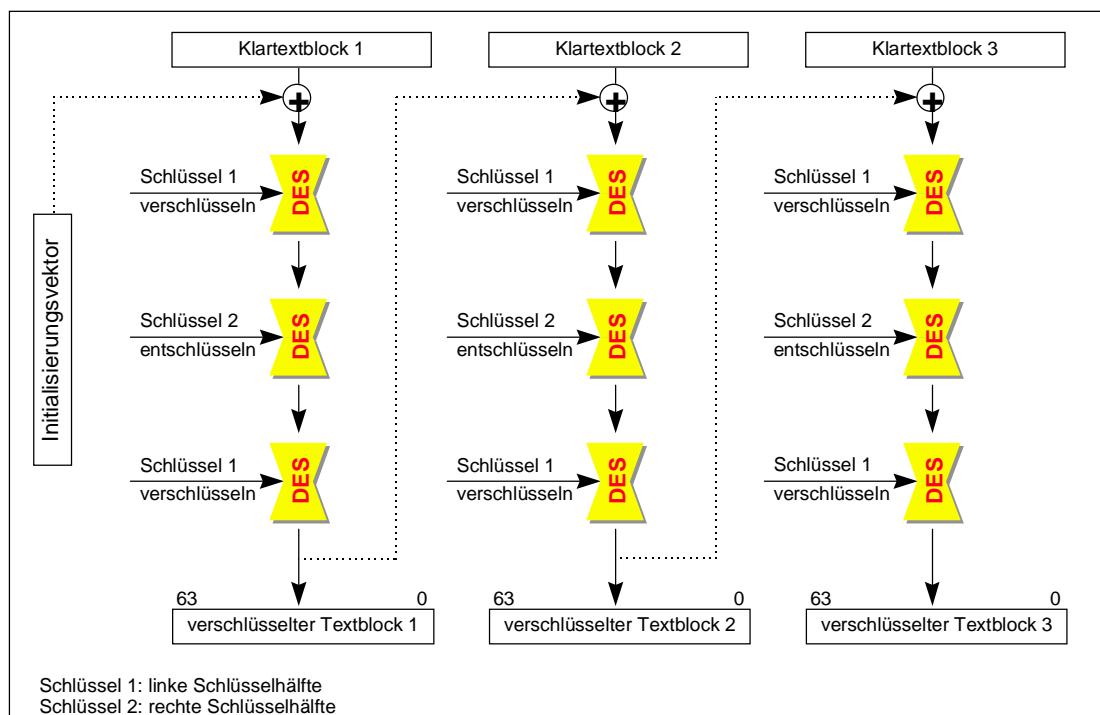


Abb. 13: 2-Key-Triple-DES im CBC-Mode

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Mechanismen	Stand: 02.02.1998	Seite: 7

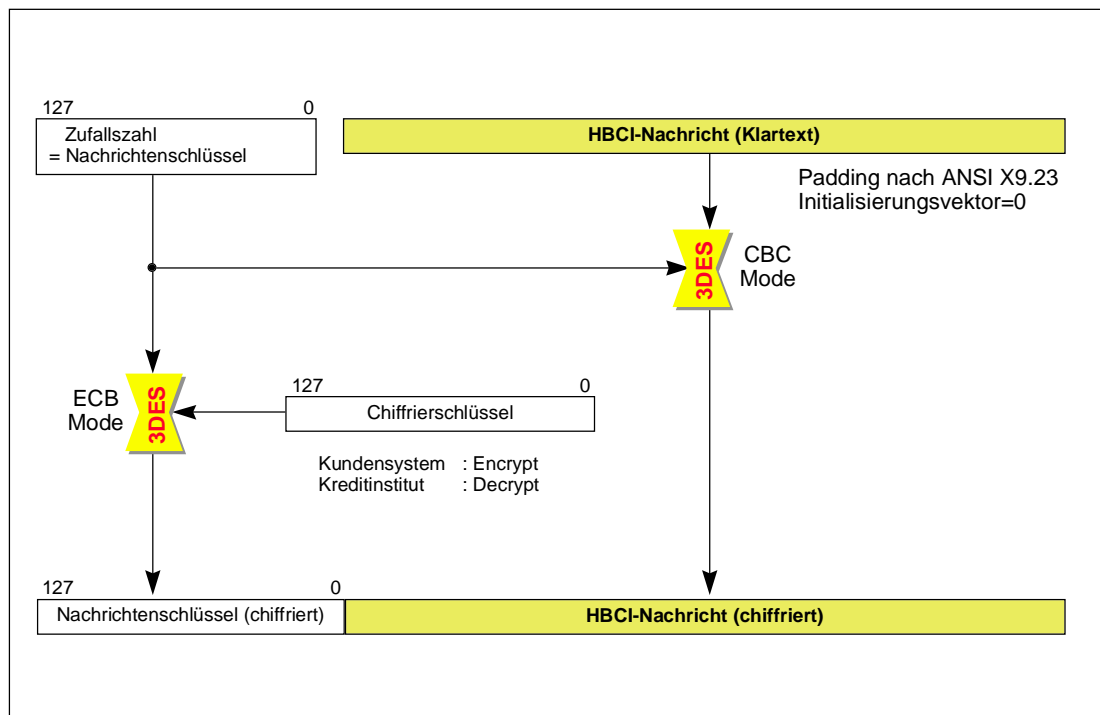


Abb. 14: Verschlüsselung bei 2-Key-Triple-DES

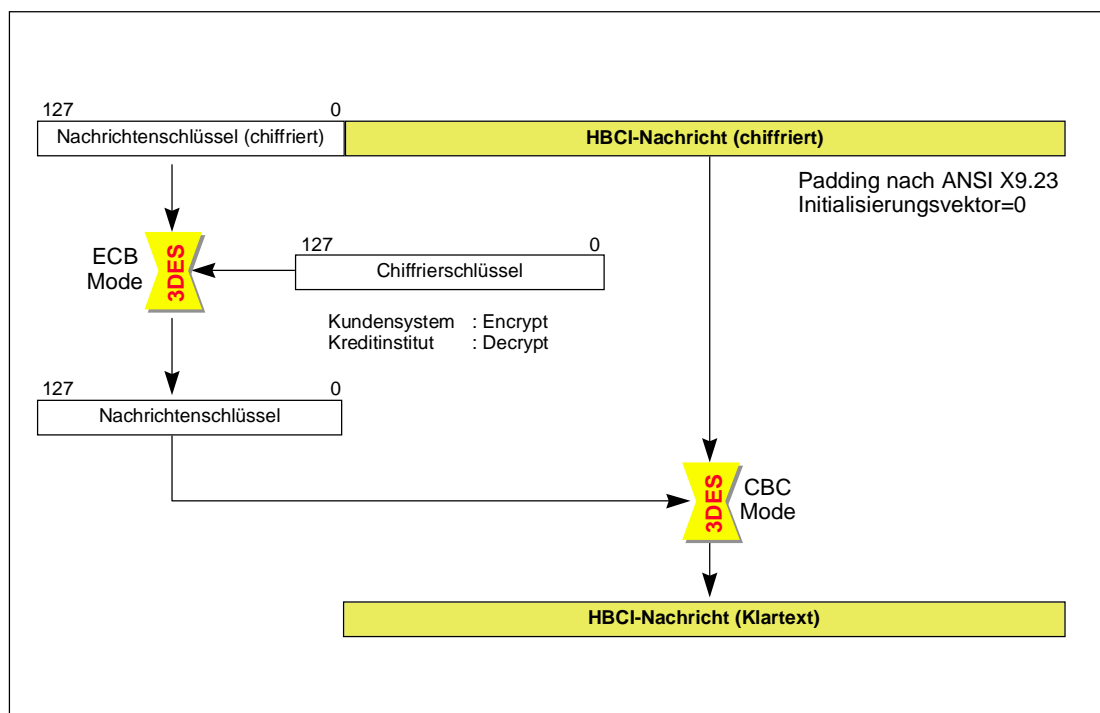


Abb. 15: Entschlüsselung bei 2-Key-Triple-DES

Die weitere Verarbeitung ist bei DDV und RDH unterschiedlich:

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 8	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Mechanismen

VI.2.2.1 Verschlüsselung bei DDV (DES-basierend)

3. Der aktuelle Nachrichtenschlüssel für die Chiffrierung der Daten wird vom Kundenprodukt mit dem kundenindividuellen Chiffrierschlüssel der Chipkarte mittels 2-Key-Triple-DES im ECB-Mode (ISO 10116) verschlüsselt (vgl. Abb. 16, sowie Abb. 14 und 15).

Aufgrund vorgegebener Verfahren bei der ZKA-Chipkarte wird zum Chiffrieren und Dechiffrieren des Nachrichtenschlüssels, unabhängig von der Übertragungsrichtung, kundensystemseitig immer die Routine „Encrypt“ benutzt, kreditinstitutsseitig immer die Routine „Decrypt“ (vgl. Kapitel VIII.8.5.3).

Realisierung Bank: optional (empfohlen)

Realisierung Kunde: optional

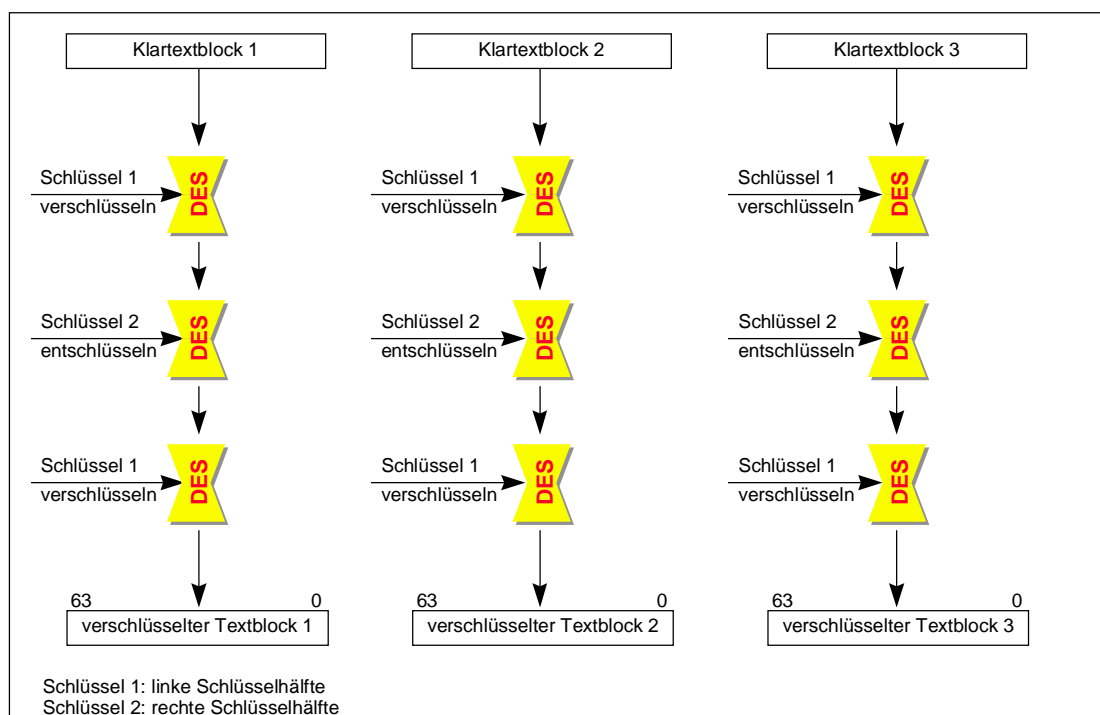


Abb. 16: 2-Key-Triple-DES im ECB-Mode

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Mechanismen	Stand: 02.02.1998	Seite: 9

VI.2.2.2 Verschlüsselung bei RDH (RSA-basierend)

- Der aktuelle Nachrichtenschlüssel wird mit dem öffentlichen Schlüssel des Empfängers chiffriert. Da die Länge des Nachrichtenschlüssels nur 16 Byte, d.h. 128 bit bei 2-Key-Triple-DES bzw. 24 Byte bei 3-Key-Triple-DES beträgt, muß er entsprechend auf 768 bit ergänzt werden, um die vorgegebene Modulslänge gemäß DFÜ-Abkommen zu erreichen. Das Padding wird mit X'00' vorgenommen, wie in Abbildung 17 gezeigt.

Realisierung Bank: verpflichtend

Realisierung Kunde: verpflichtend. Ausgenommen hiervon sind Endgeräte, die keine RDH-Verschlüsselungslösung erlauben.

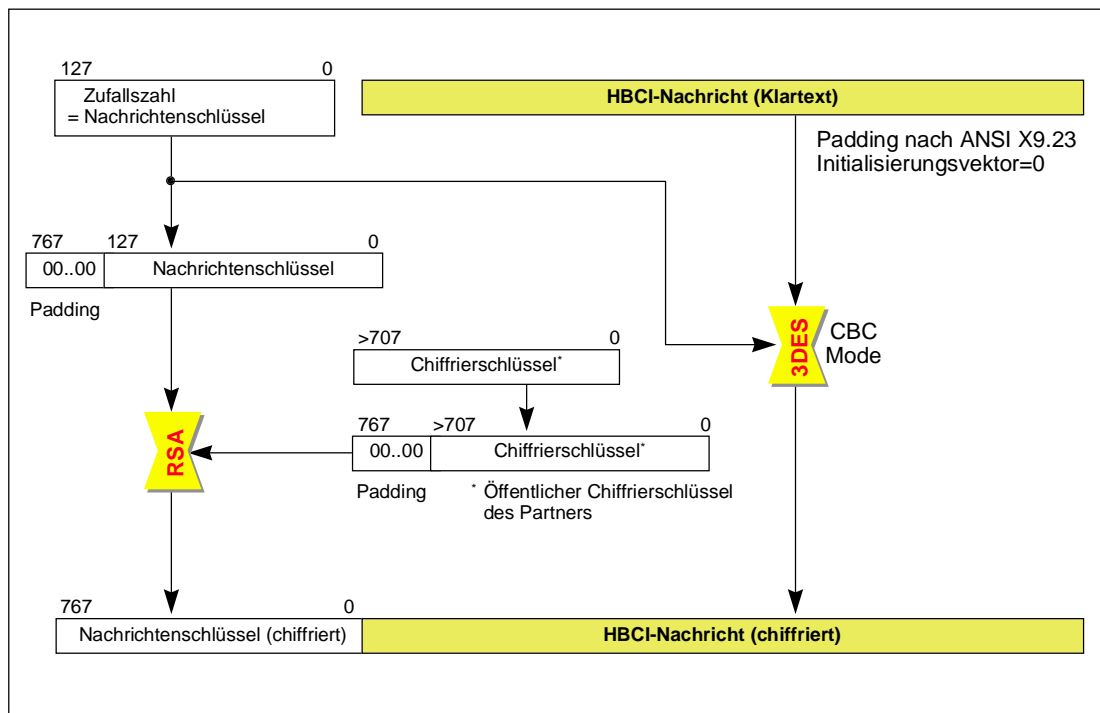


Abb. 17: Verschlüsselung bei RSA (2-Key-Triple-DES)

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 10	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Mechanismen

VI.2.3 Sicherheitsmedien beim Kundenprodukt

Bei Verwendung des symmetrischen Verfahrens (DDV) muß eine vom Kreditinstitut ausgegebene ZKA-Chipkarte eingesetzt werden, welche die Berechnung der kryptographischen Funktionen so durchführt, daß die kartenindividuellen Schlüssel niemals die Chipkarte verlassen.

Werden asymmetrische Verfahren (RDH) eingesetzt, so kann als Sicherheitsmedium eine vom Kreditinstitut ausgegebene RSA-Chipkarte oder eine Datei auf Diskette bzw. Festplatte dienen. Auf dem Sicherheitsmedium wird unter anderem der private Schlüssel des Kunden gespeichert. Es ist aber auch möglich, öffentliche Schlüssel des Kreditinstitutes darauf abzulegen oder aber im Falle einer Chipkarte die kryptographischen Operationen damit durchzuführen.



Es ist zwingend erforderlich, die Daten auf dem Sicherheitsmedium (kryptographisch) zu schützen. Speziell ist im Rahmen der Speicherung der Schlüsselpaare auf Diskette bzw. Festplatte sicherzustellen, daß die Daten unter Einbeziehung eines Paßwortes (Banking-PIN o.ä.) verschlüsselt werden und der Zugriff auf die verschlüsselten Daten nur über die manuelle Eingabe des entsprechenden Paßwortes möglich ist. [In Kürze wird hierzu ein entsprechender Vorschlag veröffentlicht.](#)

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Abläufe	Stand: 02.02.1998	Seite: 11

VI.3 Abläufe

VI.3.1 Schlüsselverwaltung

Bei der Schlüsselverwaltung muß zwischen der Verwendung von symmetrischen Schlüsseln für DDV und asymmetrischen Schlüsseln für RDH unterschieden werden.

Gemeinsam gültig sind hingegen für beide Verfahren die verwendeten Schlüsselarten, Schlüsselnamen und die Generierung von Nachrichtenschlüsseln.

VI.3.1.1 Gemeinsam verwendete Verfahren zur Schlüsselverwaltung

◆ Schlüsselarten

Grundsätzlich können Kunde und Kreditinstitut bei beiden Verfahren über zwei Schlüssel bzw. Schlüsselpaare verfügen:

- einen Signierschlüssel bzw. -schlüsselpaar
- einen Chiffrierschlüssel bzw. -schlüsselpaar

Der Signierschlüssel wird zum Unterzeichnen von Transaktionen verwendet, während der Chiffrierschlüssel zum Verschlüsseln von Nachrichten dient.

◆ Schlüsselnamen

Der Schlüsselname bei den 2-Key-Triple-DES- und RSA-Schlüsseln setzt sich aus den folgenden alphanumerischen Komponenten zusammen:

- Ländercode
(max. 3 Byte, es wird gemäß ISO 3166 der numerische Ländercode verwendet, vgl. Kapitel II.5.2)
- Kreditinstitut
(max. 30 Byte, normalerweise Bankleitzahl, vgl. Kapitel II.5.3.2)
- Benutzerkennung
(max. 30 Byte, kann vom Kreditinstitut festgelegt werden, vgl. Kapitel III.1.1)
- Schlüsselart
(1 Byte, S: Signierschlüssel; V: Chiffrierschlüssel)
- Schlüsselnummer
(max. 3 Byte)
- Versionsnummer
(max. 3 Byte)

Falls kein öffentlicher Schlüssel des Kreditinstituts vorliegt, so ist als Versionsnummer der Wert „0“ einzustellen. Damit wird kreditinstitutsseitig auf den aktuell gültigen Schlüssel referenziert. (Ein Kreditinstitut kann während einer Übergangszeit evtl. mehrere Schlüssel bis zu einem Verfallsdatum vorhalten. Aktuell gültig ist jeweils der neueste Schlüssel.)

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 12	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Abläufe

♦ Generierung von Nachrichtenschlüsseln

Zur Chiffrierung von Nachrichten wird ein dynamisch erzeugter Nachrichtenschlüssel verwendet, der folgendermaßen gebildet wird:

1. Generieren einer 16 Byte langen Zufallszahl
2. Erzeugung von ungerader Parität (optional)
3. Testen, ob erste und zweite Schlüsselhälfte unterschiedlich (optional)
4. Testen nach schwachen und semi-schwachen Schlüsseln (optional) (s. Kap. VI.2.2)

VI.3.1.2 Symmetrische Schlüssel für DDV

Für Verschlüsselung und MAC-Berechnung werden, wie unter VI.3.1.1 beschrieben, unterschiedliche Schlüssel für Signatur und Chiffrierung verwendet.

VI.3.1.2.1 Schlüsselgenerierung

Beim symmetrischen Verfahren (DDV) sind zur Bildung eines kundenindividuellen Schlüssels beim Kreditinstitut zwei Voraussetzungen zu erfüllen:

- Generierung eines ZKA-weit eindeutigen 2-Key-Triple-DES-Masterkey pro Schlüsselart und Ablegen in einer sicheren Umgebung (Hardwareeinrichtung) als Key Generating Key (KGK).
- Herleiten des jeweiligen kundenindividuellen Schlüssels mittels CID-Feld (Cardholders Information Data = Feld „EF_ID“) auf der ZKA-Chipkarte und entsprechendem 2-Key-Triple-DES-Masterkey.

♦ Generierung eines 2-Key-Triple-DES-Masterkey:

Für die Generierung von ZKA-weit einheitlichen 2-Key-Triple-DES-Masterkeys (KGK = Key Generating Key), die als Basis für die Herleitung der kundenindividuellen Signier- und Chiffrierschlüsseln dienen, ist folgendes Verfahren, analog der ZKA-Chipkarte, zu verwenden:

1. Generieren einer 16 Byte langen Zufallszahl
2. Erzeugung von ungerader Parität (optional)
3. Testen, ob erste und zweite Schlüsselhälfte unterschiedlich
4. Testen nach schwachen und semi-schwachen Schlüsseln (s. Kap. VI.2.2)

♦ Herleitung von Kartenschlüsseln:

Zur eindeutigen Herleitung der symmetrischen Signier- und Chiffrierschlüssel wird das Feld „EF_ID“ im Master File (MF) der ZKA-Chipkarte (Cardholders Information Data (CID) ohne Padding) zusätzlich übertragen (vgl. Kapitel VI.5.1.3).

Ein kartenindividueller Schlüssel KK von 16 Byte Länge wird aus

- KGK (Key Generating Key, 16 Byte)
- CID (vollständiger Inhalt von EF_ID, mit X'00' auf das nächste Vielfache von 8 Byte Länge aufgefüllt) und

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Abläufe	Stand: 02.02.1998	Seite: 13

- dem öffentlich bekannten Initialwert $I = X'52\ 52\ 52\ 52\ 52\ 52\ 52\ 52\ 25\ 25\ 25\ 25\ 25\ 25\ 25\ 25'$ (16 Byte)

zu

$$KK = P(d * KGK(H(I, CID)))$$

berechnet.

Hierbei bezeichnen

- 'P' die Funktion "Parity Adjustment" auf ungerade Parität, die wie folgt definiert ist:
Sei b_1, \dots, b_8 die Darstellung eines Byte als Folge von 8 bit. Dann setzt P das niedrigstwertige bit b_8 jedes Byte auf ungerade Parität, d.h. b_8 wird in jedem Byte so gesetzt, daß es eine ungerade Anzahl von 1 enthält.
- 'd * KGK' die 2-Key-Triple-DES-Entschlüsselung im ECB-Mode (ISO 10116) mit dem Schlüssel KGK.
- 'H' die in ISO 10118-2 definierte Hash-Funktion.

VI.3.1.2.2 Initiale Schlüsselverteilung

Die initiale Schlüsselverteilung erfolgt implizit mit der Verteilung der Chipkarte.

VI.3.1.2.3 Schlüsseländerungen

Beim symmetrischen Verfahren (DDV) ist wegen der Verknüpfung mit der Chipkarte auf elektronische Weise keine Änderung einzelner kartenindividueller Schlüssel möglich. Im Falle einer vermuteten Kompromittierung muß daher ein Kartenaustausch oder ein Ersatz aller Schlüssel und des Feldes „EF_ID“ erfolgen.

Bei einer Schlüsseländerung wird die Signatur-ID (Sequenzähler der Chipkarte) auf 1 zurückgesetzt. Die im Kreditinstitut geführte Liste der eingereichten bzw. noch nicht eingereichten Signatur-IDs (s. Doppeleinreichungskontrolle) wird gelöscht.

VI.3.1.2.4 Schlüsselverteilung nach Kompromittierung

Die Schlüsselverteilung nach einer Kompromittierung erfolgt ebenfalls mittels Vergabe einer neuen Chipkarte bzw. Ersatz aller Schlüssel und des EF-ID-Feldes. Die alte Chipkarte bzw. deren Schlüssel werden gesperrt.

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 14	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Abläufe

VI.3.1.3 Asymmetrische Schlüssel für RDH

Grundsätzlich können Kunde und Kreditinstitut beim asymmetrischen Verfahren (RDH) über zwei Schlüsselpaare verfügen:

- ein Signierschlüsselpaar
- ein Chiffrierschlüsselpaar

Der Signierschlüssel wird zum Unterzeichnen von Nachrichten verwendet, während der Chiffrierschlüssel zum Verschlüsseln von Nachrichten dient (vgl. Kapitel VI.2).

Falls ein Kreditinstitut seine Nachrichten nicht signiert, kann es auf das Signierschlüsselpaar verzichten.

VI.3.1.3.1 Schlüsselgenerierung

Die Schlüsselpaare des Kunden sind vom Kundenprodukt zu erzeugen. Die Schlüsselpaare des Kreditinstituts sind vom Kreditinstitut zu erzeugen. Die privaten Schlüssel sind jeweils geheim zu halten.

Die Schlüsselgenerierung hat gemäß dem folgenden Ablauf stattzufinden:³

1. Es wird ein konstanter öffentlicher Exponent e und ein für jeden Kunden individueller Modulus n für jedes eingesetzte RSA-Schlüsselsystem verwendet.
2. Der konstante öffentliche Exponent e wird auf die 4. Fermat'sche Primzahl festgelegt: $e = 2^{16} + 1$
3. Der Modulus n eines jeden RSA-Schlüsselsystems hat eine Länge von N Bit. Es sind keine führenden 0-Bits erlaubt, so daß auf jeden Fall gilt: $2^{N-1} \leq n < 2^N$
4. Der Zielwert für N ist 768, wobei eine aus der Suche nach starken Primzahlen resultierende Unterschreitung dieses Wertes um maximal 60 Bit zulässig ist.
5. n ist das Produkt zweier großer, zufällig ausgewählter Primzahlen p und q . Folgende Anforderungen werden an die Faktoren p und q gestellt:
 - p hat eine vorher festgelegte minimale Länge
 - $p - 1$ hat einen großen Primteiler⁴ r
 - $p + 1$ hat einen großen Primteiler s
 - $r - 1$ hat einen großen Primteiler

Die entsprechenden Forderungen werden an q gestellt.

Die Längen von p und q sollen sich um höchstens 12 Bits unterscheiden.

Bei der Wahl von p und q ist sicherzustellen, daß e kein Primfaktor von $p - 1$ oder $q - 1$ ist.

³ Das Verfahren entspricht dem des DFÜ-Abkommens.

⁴ Der Primteiler sollte dabei ungefähr der Länge des Schlüssels entsprechen.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Abläufe	Stand: 02.02.1998	Seite: 15

VI.3.1.3.2 Initiale Schlüsselverteilung

Der Kunde benötigt für das Einrichten eines neuen Zugangs folgende Initialinformationen:

- seine Benutzerkennung
- Informationen zum Kommunikationszugang

Die Übermittlung dieser Informationen ist auf zwei Wegen denkbar:

- Schriftstück des Kreditinstitutes (Benutzerkennung und Zugangsdaten müssen manuell vom Kunden eingegeben werden)
- Diskette des Kreditinstitutes mit folgendem Inhalt:
 - Segment HIUPA der UPD inkl. Benutzerkennung
 - Aktuelle Version der Zugangsdatenbank des jeweiligen Verbandes bzw. Segment HIKOM mit den Kommunikationszugangsdaten des jeweiligen Instituts

Zu Beginn muß ein gegenseitiger Austausch der öffentlichen Schlüssel von Kunde und Kreditinstitut erfolgen.⁵

Hierzu ist folgender Ablauf vorgesehen:

1. Das Kreditinstitut übermittelt seinen öffentlichen Chiffrierschlüssel an den Kunden. Falls es Nachrichten signiert, übermittelt es ebenfalls seinen öffentlichen Signierschlüssel. Hierzu gibt es zwei Möglichkeiten:
 - Zusenden bzw. Aushändigung der Schlüssel und anderer relevanter Daten auf einem Medium (z.B. Diskette⁶, Chipkarte) bei Vertragseröffnung.
Falls dem Kunden eine Diskette zugesendet wird, hat diese folgende Daten zu enthalten:
 - Datei mit ein bzw. zwei Segmenten vom Typ HIISA, die jeweils einen öffentlichen Schlüssel des Kreditinstitutes enthalten
 - BPD des Kreditinstitutes
 - Übertragung der Schlüssel beim Erstzugang
 - (1) Der Kunde fordert beide öffentlichen Schlüssel und die BPD mit Hilfe der Key-Management-Nachricht „Erstmalige Anforderung der Schlüssel des Kreditinstituts“ (s. Kap. VI.6.2.2) an. Diese Nachricht ist weder signiert noch chiffriert.
 - (2) Der weitere Ablauf ist abhängig davon, ob das Kreditinstitut seine Antwortnachrichten signiert.

⁵ Mittelfristig ist geplant, hier eine für Kunde und Kreditinstitut einfacher zu handhabende Lösung unter Einsatz von Zertifizierungsinstanzen zu erarbeiten. Derzeit wird jedoch weitgehend gemäß DFÜ-Abkommen verfahren.

⁶ Es kann sich hierbei um dieselbe Diskette handeln, mit der dem Kunden seine Benutzerkennung mitgeteilt wird (s.o.).

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 16	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Abläufe

Fall A: Das Kreditinstitut signiert

Der Kunde erhält beide Schlüssel zurückgemeldet. Während die Authentizität des Chiffrierschlüssels dabei durch die Signatur gesichert ist, ist die Authentizität des Signierschlüssels nicht gesichert, da das Kundensystem die Echtheit der Signatur noch nicht prüfen kann.

Fall B: Das Kreditinstitut signiert nicht

Der Kunde erhält nur den öffentlichen Chiffrierschlüssel zurückgemeldet. Dessen Authentizität ist dabei nicht gesichert.

- (3) Diese Nachricht muß von einem Ini-Brief an den Kunden begleitet werden. Die Gestaltung ist dem Kreditinstitut freigestellt, sollte sich aber am Muster in Abbildung 18 orientieren. Der Ini-Brief enthält für den Fall A **Exponent und Modulus des Signierschlüssels sowie dessen Hashwert** und für den Fall B **Exponent und Modulus des Chiffrierschlüssels sowie dessen Hashwert**. **Exponent und Modulus sind dabei mit führenden Nullen (X'00') auf 768 Bit zu ergänzen**. Ferner enthält **der Ini-Brief** den jeweiligen Schlüsselnamen. Bei der Hashwertbildung ist wie folgt vorzugehen:

- Padding der höchstwertigen Bits von Exponent und Modulus des Schlüssels mit Nullen (X'00') auf 1024 Bit
- Konkatenierung von Exponent und Modulus (Exponent || Modulus)
- Bildung des Hashwerts mittels RIPEMD-160 gemäß Kap. VI.2.1.1 über diesen Ausdruck

- (4) Nach Erhalt des Ini-Briefs führt der Kunde einen Vergleich des im Ini-Brief aufgeführten Hashwerts mit dem Hashwert des vom Kreditinstitut übermittelten Schlüssels durch.



Das Kundenprodukt sollte den Hashwertvergleich für den Kunden in geeigneter Weise unterstützen.

- (5) Bei Übereinstimmung der Hashwerte gelten die öffentlichen Schlüssel des Kreditinstituts als authentisiert.
- Der Kunde übermittelt seine beiden öffentlichen Schlüssel, die mit dem privaten Signierschlüssel unterzeichnet wurden, im Rahmen der Key-Management-Nachricht „Erstmalige Übermittlung der Schlüssel des Kunden“ an das Kreditinstitut (vgl. Kapitel VI.6.2.3). Diese Nachricht muß sowohl signiert als auch chiffriert sein.
 - Begleitet wird diese Nachricht durch einen Ini-Brief gemäß dem in Abbildung 18 aufgeführten Muster. Im Ini-Brief bestätigt der Kunde ausschließlich den öffentlichen Signierschlüssel mit handschriftlicher Unterschrift. Eine Bestätigung des öffentlichen Chiffrierschlüssels ist nicht erforderlich, da dieser mit dem Signierschlüssel signiert wird und damit authentifiziert ist. Neben dem Schlüssel und dem Schlüsselnamen wird im Ini-Brief der Hashwert des Schlüssels aufgeführt. Dieser wird ebenso gebildet wie der Hashwert im Ini-Brief des Kreditinstituts (s.o.).

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Abläufe	Stand: 02.02.1998	Seite: 17

4. Im Kreditinstitut findet ein Vergleich zwischen dem im Ini-Brief aufgeführten Hashwert und dem Hashwert des vom Kunden übermittelten öffentlichen Signierschlüssels statt.
5. Falls dieser Vergleich positiv verläuft, werden die öffentlichen Schlüssel des Kunden freigeschaltet und der Kunde kann Auftragsnachrichten senden.

Um die Multibankfähigkeit verschiedener Kundenprodukte zu sichern, gelten für die Ini-Diskette folgende Namenskonventionen:

- Segment HIUPA: <Benutzerkennung>.UPA
- Datei mit den öffentlichen Schlüsseln: <Benutzerkennung>.PKD
- BPD: <Bankleitzahl>.BPD
- Segment mit Kommunikationszugang: <Bankleitzahl>.KOM
- Zugangsdatenbank des Verbandes: BDB.KOM, BVR.KOM, DSGVO.KOM bzw. VOEB.KOM

Falls die Benutzerkennung nicht im Dateisystem darstellbar ist, ist sie entsprechend zu kürzen. Die Diskette muß im Standardformat des jeweiligen Betriebssystems formatiert sein. Die Dateien sind im Stammverzeichnis der Diskette abzulegen.

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 18	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Abläufe

Ini-Brief

Benutzername	System	Kundensoftware-interner Name (Angabe freigestellt)
Datum	TT.MM.JJ	Datum der Erstellung des Initialisierungsauftrags
Uhrzeit	hh:mm	Uhrzeit der Erstellung des Initialisierungsauftrags
Empfänger		Kreditinstitutskennung (wird vom jeweiligen Kreditinstitut mitgeteilt)
Benutzerkennung		max. 30 Stellen alphanumerisch (wird vom jeweiligen Kreditinstitut mitgeteilt)
Schlüsselnummer		Nummer des Signierschlüssels (max. 3 Stellen)
Schlüsselversion		Version des Signierschlüssels (max. 3 Stellen)
HBCI-Version	2.0	

Öffentlicher Schlüssel für die elektronische Signatur:

Exponent 0768

```

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01

```

Modulus 0768

```

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
99 8C 2A 20 20 5E 96 98 4B 3D 35 3B 9B 9B 34 AB
A4 BB 79 8C 31 41 2E 75 AE EE F5 E2 9F B4 08 17
9F B8 93 7D 8B E4 ED A6 93 80 B8 80 FD 5D 3A 9A
44 26 C0 AD 09 4A 86 BB BD C9 75 98 C5 0F B8 A2
D0 9F 95 B7 9C 54 01 F6 79 46 24 42 83 FE 96 26
73 0B 6A EF 89 F9 3D 04 8A 98 96 7A 56 78 81 07

```

Hash D2 FD 56 F3 1E 5C 76 D2 B8 2C
0B 1E 4C 6A 13 9E 85 87 E8 D3

Ich bestätige hiermit den obigen öffentlichen Schlüssel für meine elektronische Signatur.

Ort / Datum

Unterschrift

Abb. 18: Beispiel für die Gestaltung des Ini-Briefs

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Abläufe	Stand: 02.02.1998	Seite: 19

VI.3.1.3.3 Schlüsseländerungen

◆ Routinemäßige Schlüsseländerung des Kunden

Ein Kunde ändert seine Signier- und Chiffrierschlüsselpaare unabhängig.

Der Kunde sendet je Kreditinstitut im Rahmen eines HBCI-Dialoges eine Nachricht, in welcher dieses über einen neuen öffentlichen Schlüssel informiert wird (vgl. Kapitel VI.6.2.1). Die Nachricht ist mit dem alten (bei Wechsel des Signierschlüssels), respektive dem aktuellen (bei Wechsel des Chiffrierschlüssels) privaten Signierschlüssel des Kunden zu signieren. Analog dazu ist die Nachricht mit dem alten Chiffrierschlüssel zu chiffrieren. Das Kreditinstitut speichert diesen neuen öffentlichen Schlüssel des Kunden und verwendet ihn **ab sofort (d.h. bereits in der Antwortnachricht)** für alle Verschlüsselungen bzw. Verifikationen von Signaturen.

Falls die Übermittlung der neuen Schlüssel aus irgendeinem Grunde fehlschlägt, kann der Kunde den Vorgang beliebig wiederholen.

Bei einer Schlüsseländerung wird die Signatur-ID auf 1 zurückgesetzt. Die Liste der eingereichten bzw. noch nicht eingereichten Signatur-IDs (s. Doppeleinreichungskontrolle) wird gelöscht.

◆ Routinemäßige Schlüsseländerung des Kreditinstituts

Ein Kreditinstitut generiert bei Bedarf ein neues Schlüsselpaar.

Der Kunde sendet jeweils bei der Dialoginitialisierung die Referenz auf die öffentlichen Schlüssel des Kreditinstitutes mit (vgl. Kapitel III.3.1). Falls das Kreditinstitut über aktuellere öffentliche Schlüssel verfügt, werden diese in der Kreditinstitutsnachricht mitübertragen (vgl. Kapitel III.3.2 respektive VI.6.1.3).

Zur Verifikation des kreditinstitutsseitigen öffentlichen Schlüssels auf dem Kundensystem kann das entsprechende Kreditinstitut die Kreditinstitutsnachricht mit dem alten Signierschlüssel signieren (wenn eine kreditinstitutsseitige Signatur vorgesehen ist) oder den Hashwert des öffentlichen Schlüssels analog der initialen Schlüsselverteilung an den Kunden übermitteln. Die Verifikation ist grundsätzlich optional.

Nach Ablauf einer festgelegten Frist akzeptiert dann das Kreditinstitut Nachrichten nicht mehr, die mit ihrem alten öffentlichen Schlüssel chiffriert wurden.

VI.3.1.3.4 Schlüsselverteilung nach Kompromittierung

Die Verteilung der Schlüssel nach einer Kompromittierung erfolgt analog der Schlüsselverteilung bei der Initialisierung. Ein Austausch beider Schlüssel findet auch dann statt, wenn nur einer der beiden Schlüssel kompromittiert wurde.

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 20	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Abläufe

VI.3.2 Doppeleinreichungskontrolle

Die Doppeleinreichungskontrolle wird mittels eines Zählers pro Signatur realisiert (Signatur-ID), dessen Inhalt jeweils in die Signatur(en) der Nachricht einfließt (Verfahrensbeschreibung siehe Kapitel VI.4).

VI.3.3 Schlüsselsperrung

Bei der Schlüssel- bzw. Benutzersperrung muß zwischen folgenden Fällen unterschieden werden:

- Kompromittierung des eigenen Schlüssels
- Verlust des eigenen Schlüssels
- Überschreiten der Anzahl der Falschsignaturen

Zusätzlich müssen bei der Sperrung noch folgende Punkte berücksichtigt werden:

- Information des Kunden
- Entsperrung

Die Sperrung anderer Benutzer wird als eigenständiger Auftrag behandelt und zu einem späteren Zeitpunkt realisiert.

◆ Kompromittierung des eigenen Schlüssels

Bei Verdacht auf Kompromittierung des eigenen Schlüssels kann die Sperrung mittels einer speziellen Nachricht (vgl. Kapitel VI.6.2.4) erfolgen, welche signiert sein muß.

◆ Verlust des eigenen Schlüssels

Bei einem Verlust (inkl. Diebstahl) des eigenen Schlüssels (respektive des Speichermediums) muß der Kunde Schlüssel bzw. Medium sperren und beim Kreditinstitut ein anderes Medium inkl. Schlüssel beantragen.

Eine nicht-signierungspflichtige Sperrmöglichkeit ist optional, da hierdurch die Gefahr des Mißbrauchspotential gegeben ist (absichtliche Sperrung fremder Anschlüsse). Der Segmentaufbau erfolgt analog der oben beschriebenen Nachricht, jedoch ist keine Signatur nötig (möglich). Die Steuerung hierfür erfolgt über das Feld „Anzahl benötigter Signaturen“ in der UPD.

Eine Sperrung auf anderem Weg (z.B. telefonische Sperrung über Servicezentralen) muß immer möglich sein (z.B. Verlust der eigenen Infrastruktur).

◆ Überschreiten der Anzahl der Falschsignaturen

Wird beim Einreichen von Aufträgen durch fehlerhafte Signaturen die festgelegte Anzahl von Falschsignaturen überschritten, wird kreditinstitutsseitig der Schlüssel gesperrt.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Abläufe	Stand: 02.02.1998	Seite: 21

◆ Information des Kunden

Im Falle einer Sperrung aufgrund von Schlüsselkompromittierung oder Schlüsselverlust erhält der Kunde auf die Sperrnachricht eine Antwortnachricht (vgl. Kapitel VI.2.4 b), welche ihm die Sperrung bestätigt. Bei einer Sperrung wegen Überschreitung des Maximalwertes möglicher Falschsignaturen erhält er lediglich einen entsprechenden Rückmeldungscode. In jedem Fall erhält er jedoch entsprechende Fehlermeldungen bei der Einreichung nachfolgender Nachrichten.

◆ Entsperrung

Eine Entsperrung erfolgt nur gegen handschriftliche Unterschrift des Kunden.

Ist der Schlüssel kompromittiert oder nicht mehr auffindbar, so wird für den Benutzer eine neue Chipkarte, respektive neue Schlüssel und ein neues EF_ID (DDV), oder ein neues Schlüsselpaar (RDH) erzeugt und der alte Schlüssel bleibt gesperrt. Es werden in jedem Falle beide Schlüsselpaare neu vergeben, auch wenn nur ein Schlüsselpaar kompromittiert sein sollte.

In den übrigen Fällen kann der Schlüssel einfach durch das Kreditinstitut entsperrt werden.

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 22	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Bankfachliche Anforderungen

VI.4 Bankfachliche Anforderungen

◆ Zu signierende Nachrichten

Grundsätzlich sind alle Kundennachrichten zu signieren. Ausnahmen gelten beim anonymen Zugang, bei der Erstinitialisierung und der Schlüsselsperrung.

Die Signatur von Kreditinstitutsnachrichten ist optional.

◆ Doppeleinreichungskontrolle

Bei der Doppeleinreichungskontrolle (Verhinderung von Replay-Attacken) ist zu berücksichtigen, daß die sequentiell erzeugten Referenznummern (=Signatur-IDs) beim Kreditinstitut nicht in derselben Reihenfolge eintreffen müssen, da diese kundenseitig auch offline (d.h. zeitlich voneinander unabhängig) generiert werden können. Das Kreditinstitut muß deshalb sicherstellen, daß innerhalb eines bestimmten Zeitraums keine Sequenznummer mehrfach erscheint.

Aus diesem Grund muß beim Kreditinstitut eine Liste mit den eingereichten (Positivliste) oder noch nicht eingereichten (Negativliste) Signatur-IDs geführt werden. Nach einer festgelegten Aufbewahrungsfrist wird eine Referenznummer nicht mehr akzeptiert. (Konkret wird ein Kreditinstitut eine Nachricht abweisen, welche länger als die vereinbarte Frist nach einer Nachricht mit höherer Signatur-ID eintrifft).

◆ Mehrfachsignaturen

Bei Mehrfachsignaturen kann unterschieden werden, ob die Reihenfolge der Unterzeichnung bedeutungslos oder relevant ist. Diese Unterscheidung muß nicht nur im Kundenprodukt gemacht werden können, sondern hat auch Einfluß auf die Verarbeitung und Kontrolle im Kreditinstitut. In der vorliegenden HBCI-Version ist die Reihenfolge der Signaturen bedeutungslos.

Sind die Berechtigungsprofile mehrerer signierender Benutzer zueinander inkonsistent, so liegt es im Ermessen des Kreditinstituts, ob es die Nachricht annimmt oder ablehnt (Bsp.: Der Erfasser einer Nachricht, für deren Aufträge drei Signaturen erforderlich sind, liefert nur eine zweite Signatur eines Benutzers mit, der über das Recht verfügt, die Aufträge alleine zu signieren).

Ob es zulässig ist, daß bei Mehrfachsignaturen verschiedene Signaturverfahren eingesetzt werden, gibt das Kreditinstitut in den BPD im Segment „Sicherheitsverfahren“ (Kap. IV.4) an.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung	Stand: 02.02.1998	Seite: 23

VI.5 Formate für Signatur und Verschlüsselung

Für die Speicherung der Sicherheitsinformationen für die Signatur(en) werden unmittelbar nach dem Nachrichtenkopf das (die) Segment(e) „Signaturkopf“ (HNSHK) und unmittelbar vor dem Nachrichtenabschluß das (die) Segment(e) „Signaturabschluß“ (HNSHA) in die bestehende Nachricht eingeschoben.

Dies entspricht dem in UN/EDIFACT definierten Vorgehen und kann folgendermaßen visualisiert werden:

HNHBK	HNSHK	HBCI-Nutzdaten	HNSHA	HNHBS
-------	-------	----------------	-------	-------

(Die grau hinterlegten Bereiche gehen in die Signatur mit ein.)

Falls mehrere Signaturen für HBCI-Nachrichten erforderlich sind, so wiederholen sich Signaturkopf und -abschluß entsprechend:

HNHBK	HNSHK ₂	HNSHK ₁	HBCI-Nutzdaten	HNSHA ₁	HNSHA ₂	HNHBS
-------	--------------------	--------------------	----------------	--------------------	--------------------	-------

(Die grau hinterlegten Bereiche bezeichnen die Daten für die Zweit-Signatur bei beliebiger Reihenfolge der Signaturen (vgl. Kapitel VI.4)).

Bei der Verschlüsselung wird nach dem Nachrichtenkopf ein Verschlüsselungskopf-Segment (HNVSK) eingefügt. Dies bedeutet, daß alle Daten nach dem Segmentendekennzeichen des Nachrichtenkopfes bis zum letzten Byte vor dem Nachrichtenabschluß inklusive aller Signaturen in die Verschlüsselung eingehen:

HNHBK	HNVSK	$e_k(\text{HNSHK}_n \mid \text{HBCI-Nutzdaten} \mid \text{HNSHA}_n)$	HNHBS
-------	-------	--	-------

Grundsätzlich erfolgt die Reihenfolge der Sicherheitsverarbeitung in folgender Reihenfolge:

1. elektronische Signatur
2. evtl. Zweit- und Drittsignatur
3. (Komprimierung) und Verschlüsselung

Für die Übermittlung der sicherheitsrelevanten Informationen werden die folgenden Segmente und Datenelementgruppen übertragen.

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 24	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung

VI.5.1 Mehrfach verwendete Datenelementgruppen

VI.5.1.1 Schlüsselname

◆ Beschreibung

Die DEG enthält den Schlüsselnamen in strukturierter Form. Damit kann die Referenz auf einen Schlüssel hergestellt werden.

◆ Format

Name: Schlüsselname
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Kreditinstitut	GDG	kik	#	M	1	
2	Benutzerkennung	GD	id	#	M	1	
3	Schlüsselart	GD	an	1	M	1	B, S, V
4	Schlüsselnummer	GD	num	..3	M	1	
5	Schlüsselversion	GD	num	..3	M	1	

◆ Erläuterungen

Nr. 1: Kreditinstitutskennung

In diesem „mehrfach verwendeten HBCI-Element“ werden Kreditinstituts-[kennung](#) (Bankleitzahl) und Länderschlüssel abgespeichert (vgl. Kapitel II.5.3.2).

Nr. 2: Benutzerkennung

Das DE enthält bei Schlüsseln des Kunden die Benutzerkennung (vgl. Kapitel V.2), mit der der Kunde eindeutig identifiziert werden kann.

Bei Schlüsseln des Kreditinstituts ist eine beliebige Kennung einzustellen, die dazu dient, den Kreditinstitutsschlüssel eindeutig zu identifizieren. Diese Kennung darf nicht einer anderen gültigen Benutzerkennung des Kreditinstituts entsprechen.

Nr. 3: Schlüsselart

Die Schlüsselart steht bei RDH in engem Zusammenhang mit dem Datenelement "Verwendungszweck für öffentlichen Schlüssel" in der DEG "Öffentlicher Schlüssel" (vgl. Kapitel VI.5.1.5). Die Inhalte sind konsistent zu halten.

Abhängig vom Verwendungszweck kann die Schlüsselart drei Werte annehmen:

- „S“ für Signierschlüssel
- „V“ für Chiffrierschlüssel
- „B“ für beide

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung	Stand: 02.02.1998	Seite: 25

Nr. 4: Schlüsselnummer

Enthält die Schlüsselnummer des entsprechenden Schlüssels. Bei einer Sperrung aufgrund Verlusts des Sicherheitsmediums ist die spezielle, in Kap. VI.6.2.4 beschriebene Belegung zu beachten.

Nr. 5: Schlüsselversion

Enthält die Versionsnummer des entsprechenden Schlüssels. Bei einer Sperrung aufgrund Verlusts des Sicherheitsmediums ist die spezielle, in Kap. VI.6.2.4 beschriebene Belegung zu beachten.

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 26	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung

VI.5.1.2 Sicherheits-/Gültigkeitsdatum und -uhrzeit

◆ Beschreibung

Enthält einen Zeitstempel, sowie dessen Bedeutung.

◆ Format

Name: Sicherheitsdatum und -uhrzeit

Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Datum- und Zeitbezeichner, kodiert	GD	an	..3	M	1	1, 6
2	Datum	GD	dat	#	K	1	
3	Uhrzeit	GD	tim	#	K	1	

◆ Erläuterungen

Nr. 1: Datum- und Zeitbezeichner, kodiert

Enthält die Bedeutung des Zeitstempels. Folgende Werte sind derzeit möglich:

- „1“ für STS, Sicherheitszeitstempel
- „6“ für CRT, Certificate Revocation Time

Nr. 2: Datum

„abgeleitetes Format“ (vgl. Kapitel II.5.2)

Nr. 3: Uhrzeit

„abgeleitetes Format“ (vgl. Kapitel II.5.2)

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung	Stand: 02.02.1998	Seite: 27

VI.5.1.3 Sicherheitsidentifikation, Details

◆ Beschreibung

Die Sicherheitsidentifikation enthält nähere Angaben über die involvierten Parteien. Sie wird verwendet, um die CID (=EF_ID) bei DDV (vgl. Kapitel VI.3.1.2 bzw. VIII.8) oder die Kundensystem-ID bei RDH (vgl. Kapitel III.3.1.2) zu übertragen.

◆ Format

Name: Sicherheitsidentifikation, Details
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Bezeichner für Sicherheitspartei	GD	an	..3	M	1	1, 2
2	CID	GD	bin	..256	K	1	
3	Identifizierung der Partei	GD	id	#	K	1	

◆ Erläuterungen

Die Gruppendatenelemente Nr. 2 bzw. 3 müssen alternativ gefüllt sein.

Nr. 1: Bezeichner für Sicherheitspartei

Identifikation der Funktion der beschriebenen Partei, in diesem Falle des Kunden.

Es sind folgende Werte vorgesehen:

- "1" für 'MS' (Message Sender), wenn ein Kunde etwas an sein Kreditinstitut sendet.
- "2" für 'MR' (Message Receiver), wenn das Kreditinstitut etwas an seinen Kunden sendet.

Nr. 2: CID

Identifikation des verwendeten Schlüssels (CID, EF_ID) für DDV. Bei Verwendung des DDV-Verfahrens ist die Belegung zwingend erforderlich, bei RDH darf das Feld nicht belegt werden.

Nr. 3: Identifizierung der Partei

Code, welcher die Partei identifiziert. Bei Verwendung des RDH-Verfahrens ist [die Kundensystem-ID einzustellen, sofern diese verwendet wird.](#) Bei DDV darf das Feld nicht belegt werden.

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 28	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung

VI.5.1.4 Zertifikat

◆ Beschreibung

Bei einem späteren Einsatz von Zertifizierungsinstanzen werden im Rahmen von HBCI-Nachrichten auch Zertifikate transparent verschickt. Diese werden durch Zertifikatstyp und -inhalt beschrieben.

Da Zertifikate Informationen beinhalten, die auch in den HBCI-Formaten enthalten sind (z.B. Zertifikatsreferenz respektive Schlüsselnamen), können Daten redundant vorkommen. Diese müssen dann auf Konsistenz überprüft werden, bei Unstimmigkeiten hat das Zertifikat Vorrang.

◆ Format

Name: Zertifikat
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Zertifikatstyp	GD	num	1	M	1	1, 2, 3
2	Zertifikatsinhalt	GD	bin	.. 2048	M	1	

◆ Erläuterungen

Nr. 1: Zertifikatstyp

Kennzeichnet Aufbau und Inhalt des Zertifikats.

Es sind folgende Werte vorgesehen:

- "1" für ZKA
- "2" für UN/EDIFACT
- "3" für X.509

Nr. 2: Zertifikatsinhalt

Hier wird das Zertifikat selbst transparent eingestellt.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung	Stand: 02.02.1998	Seite: 29

VI.5.1.5 Öffentlicher Schlüssel

◆ Beschreibung

Dieses Format wird nur bei RDH-Key-Management verwendet und dient zum Transport des öffentlichen Schlüssels zwischen Kunde und Kreditinstitut bzw. umgekehrt.

◆ Format

Name: Öffentlicher Schlüssel
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Verwendungszweck für öffentlichen Schlüssel	GD	an	..3	M	1	5, 6
2	Operationsmodus, kodiert	GD	an	..3	M	1	16
3	Verfahren Benutzer	GD	an	..3	M	1	10
4	Wert für Modulus	GD	bin	..512	M	1	
5	Bezeichner für Modulus	GD	an	..3	M	1	12
6	Wert für Exponent	GD	bin	..512	M	1	65537
7	Bezeichner für Exponent	GD	an	..3	M	1	13

◆ Erläuterungen

Nr. 1: Verwendungszweck für öffentlichen Schlüssel

Kennzeichnet den Verwendungszweck für den öffentlichen Schlüssel. Diese Information muß konsistent zum Datenelement „Schlüsselart“ im Segment „Schlüsselname“ (vgl. Kapitel VI.5.1.1) gehalten werden.

Es sind folgende Werte vorgesehen:

- "5" für OCF, Owner Ciphering (Chiffrierschlüssel)
- "6" für OSG, Owner Signing (Signierschlüssel)

Nr. 2: Operationsmodus, kodiert

Es ist folgender Wert vorgesehen:

- "16" für DSMR (ISO 9796)

Nr. 3: Verfahren Benutzer

Es sind folgende Werte zugelassen:

- "10" für RSA

Nr. 4: Wert für Modulus

Enthält den Modulus des öffentlichen Schlüssels.

Nr. 5: Bezeichner für Modulus

Enthält den Bezeichner für „Modulus“.

- "12" für MOD, Modulus

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 30	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung

Nr. 6: Wert für Exponent

Der Wert für den Exponenten des öffentlichen Schlüssels ist

- "65537"

Nr. 7: Bezeichner für Exponent

Enthält den Bezeichner für „Exponent“.

- "13" für EXP, Exponent

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung	Stand: 02.02.1998	Seite: 31

VI.5.2 Signaturkopf

VI.5.2.1 Segmentbeschreibung

◆ Beschreibung

Der Signaturkopf enthält Information über den damit verbundenen Sicherheitsservice, sowie über den Absender.

◆ Format

Name: Signaturkopf
 Typ: Segment
 Segmentart: Administration
 Kennung: HNSHK
 Bezugssegment: -
 Segmentversion: 3
 Sender: Kunde/Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Sicherheitsfunktion, kodiert	DE	an	..3	M	1	1, 2
3	Sicherheitskontrollreferenz	DE	an	..14	M	1	<>0
4	Bereich der Sicherheitsapplikation, kodiert	DE	an	..3	M	1	1
5	Rolle des Sicherheitslieferanten, kodiert	DE	an	..3	M	1	1, 3, 4
6	Sicherheitsidentifikation, Details	DEG			M	1	
7	Sicherheitsreferenznummer	DE	num	..16	M	1	
8	Sicherheitsdatum und -uhrzeit	DEG			M	1	
9	Hashalgorithmus	DEG			M	1	
10	Signaturalgorithmus	DEG			M	1	
11	Schlüsselname	DEG			M	1	
12	Zertifikat	DEG			K	1	

◆ Erläuterungen

Nr. 2: Sicherheitsfunktion, kodiert

Spezifiziert die auf die Nachricht angewendete Sicherheitsfunktion.

Im Zusammenhang mit elektronischen Signaturen sind folgende Werte möglich:

- „1“ für NRO, Non-Repudiation of Origin (für RDH)
- „2“ für AUT, Message Origin Authentication (für DDV)

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 32	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung

Nr. 3: Sicherheitskontrollreferenz

Die Sicherheitskontrollreferenz stellt die Verbindung zwischen Signaturkopf und dazu gehörigem Signaturabschluß (s. Kap. VI.5.3) her. Sie muß mit dem entsprechenden Feld im Signaturabschluß übereinstimmen.

Nr. 4: Bereich der Sicherheitsapplikation, kodiert

Definiert, welche Daten vom kryptographischen Prozeß verarbeitet werden. Wird benötigt um z.B. zwischen relevanter und belangloser Reihenfolge von Signaturen zu unterscheiden (vgl. Kapitel VI.4).

Es sind folgende Werte möglich:

- "1" für SHM (Signaturkopf und HBCI-Nutzdaten)
- "2" für SHT (von Signaturkopf bis Signaturabschluß)

Wenn SHM gewählt wird, so bedeutet dies, daß nur über den eigenen Signaturkopf sowie die HBCI-Nutzdaten ein Hashwert gebildet wird, der in die Signatur eingeht. Dies entspricht bei Mehrfachsignaturen einer bedeutungslosen Reihenfolge.

Wenn SHT gewählt wird, dann werden auch alle schon vorhandenen Signaturköpfe und -abschlüsse mitsigniert. Das heißt, daß die Reihenfolge der Signaturen relevant ist.

Der einzig zugelassene Wert ist "1", d.h. SHM.

Nr. 5: Rolle des Sicherheitslieferanten, kodiert

Beschreibt das Verhältnis desjenigen, der die Sicherheit gewährleistet, bezüglich der zu sichernden Nachricht.

Es sind folgende Werte möglich:

- "1" für ISS, Herausgeber der signierten Nachricht (z.B. Erfasser oder Erstschrift)
- "3" für CON, der Unterzeichnete unterstützt den Inhalt der Nachricht (z.B. bei Zweitschrift)
- "4" für WIT, der Unterzeichnete ist Zeuge (z.B. Übermittler), aber für den Inhalt der Nachricht nicht verantwortlich

Die Wahl ist von der bankfachlichen Auslegung der Signatur, respektive vom vertraglichen Zustand zwischen Kunde und Kreditinstitut abhängig.

Nr. 6: Sicherheitsidentifikation, Details

Identifikation der im Sicherheitsprozeß involvierten Parteien. Dient zur Übermittlung der CID im DDV-Verfahren bzw. der Kundensystem-ID im RDH-Verfahren.

Details siehe VI.5.1.3

Nr. 7: Sicherheitsreferenznummer

Sicherheitsrelevante Nachrichtenidentifikation (Signatur-ID), welche zur Verhinderung der Doppeleinreichung, respektive Garantie der Nachrichtensequenzintegrität eingesetzt werden kann.

Bei chipkartenbasierten Verfahren ist der Sequenzzähler der Chipkarte (s. Kap. VIII.8.2.9) einzustellen. Bei softwarebasierten Verfahren wird die Si-

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung	Stand: 02.02.1998	Seite: 33

cherheitsreferenznummer auf Basis der Kundensystem-ID und des Schlüsselnamens (Benutzerkennung) verwaltet.

Nr. 8: Sicherheitsdatum und -uhrzeit

Gibt Datum und Uhrzeit des lokalen Rechners an, an dem die Unterschrift geleistet wurde. Als Bedeutung wird „1“ eingestellt, da es sich um einen Sicherheitszeitstempel handelt.

Details siehe VI.5.1.2

Nr. 9: Hashalgorithmus

Enthält einen kryptographischen Algorithmus, seinen Operationsmodus, sowie dessen Einsatz.

Details siehe VI.5.2.2

Nr. 10: Signaturalgorithmus

Enthält einen kryptographischen Algorithmus, seinen Operationsmodus, sowie dessen Einsatz.

Details siehe VI.5.2.3

Nr. 11: Schlüsselname

Enthält den verwendeten Schlüsselnamen, respektive die Referenz auf den Schlüssel.

Details siehe VI.5.1.1

Nr. 12: Zertifikat

Hier wird bei späterem Einsatz von Zertifizierungsinstanzen ein Zertifikat transparent eingestellt.

Details siehe VI.5.1.4

◆ Beispiel

```
HNSHK:2:3+1+654321+1+1+1::2+3234+1:19960605:1111
44+1:999:1+6:10:16+280:10020030:12345:S:1:1'
```

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 34	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung

VI.5.2.2 Hashalgorithmus

◆ Beschreibung

Enthält einen kryptographischen Algorithmus, seinen Operationsmodus, so wie dessen Einsatz, in diesem Fall für RIPEMD-160 als verwendeter Hashalgorithmus.

◆ Format

Name: Hashalgorithmus
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Verwendung des Hashalgorithmus, kodiert	GD	an	..3	M	1	1
2	Hashalgorithmus, kodiert	GD	an	..3	M	1	999
3	Bezeichner für Hashalgorithmusparameter	GD	an	..3	M	1	1
4	Wert des Hashalgorithmusparameters	GD	bin	..512	K	1	

◆ Erläuterungen

Nr. 1: Verwendung des Hashalgorithmus, kodiert

Spezifiziert die Verwendung des in Feld 2 identifizierten Algorithmus.

Im Zusammenhang mit Hash-Funktionen ist derzeit nur folgender Wert möglich:

- "1" für OHA, Owner Hashing

Nr. 2: Hashalgorithmus, kodiert

Spezifiziert den verwendeten Hash-Algorithmus:

- "999" für ZZZ, gegenseitig vereinbart (RIPEMD-160).

Nr. 3: Bezeichner für Hashalgorithmusparameter

Dies bedingt den folgenden Wert:

- "1" für IVC, Initialization value, cleartext

Nr. 4: Wert des Hashalgorithmusparameters

Bei RIPEMD-160 wird folgender Initialisierungswert als Default verwendet: X'67 45 23 01 EF CD AB 89 98 BA DC FE 10 32 54 76 C3 D2 E1 F0'.

In einer zukünftigen Version kann dieses DE mit einem abweichenden Initialisierungswert belegt werden. Zur Zeit ist die Belegung nicht zulässig.

◆ Beispiel

1:999:1

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung	Stand: 02.02.1998	Seite: 35

VI.5.2.3 Signaturalgorithmus

◆ Beschreibung

Enthält einen kryptographischen Algorithmus, seinen Operationsmodus, so wie dessen Einsatz, in diesem Fall für die Signaturbildung über DDV bzw. RDH.

◆ Format

Name: Signaturalgorithmus
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Verwendung des Signaturalgorithmus, kodiert	GD	an	..3	M	1	6
2	Signaturalgorithmus, kodiert	GD	an	..3	M	1	1, 10
3	Operationsmodus, kodiert	GD	an	..3	M	1	16, 999

◆ Erläuterungen

Nr. 1: Verwendung des Signaturalgorithmus, kodiert

Spezifiziert die Verwendung des in Feld 2 identifizierten Algorithmus.

Im Zusammenhang mit Signaturbildung ist derzeit nur folgender Wert möglich:

- "6" für OSG, Owner Signing

Nr. 2: Signaturalgorithmus, kodiert

Verfahren bezogen auf die Verwendung der Signatur.

Es sind folgende Werte vorgesehen:

- "1" für DES (bei DDV)
- "10" für RSA (bei RDH)

Nr. 3: Operationsmodus, kodiert

Spezifiziert den verwendeten Operationsmodus.

Es sind folgende Werte vorgesehen (vgl. Kapitel VI.2.1):

- "16" für DSMR, Digital Signature Scheme giving Message Recovery: ISO 9796 (bei RDH)
- "999" für ZZZ, gegenseitig vereinbart (bei DDV bedeutet dies die Bildung eines Retail-MAC für die Berechnung der Signatur)

◆ Beispiel

6:10:16

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 36	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung

VI.5.3 Signaturabschluß

◆ Beschreibung

Der Signaturabschluß stellt die Verbindung mit dem dazugehörigen Signaturkopf her und enthält als "Validierungsergebnis" die elektronische Signatur.

◆ Format

Name: Signaturabschluß
Typ: Segment
Segmentart: Administration
Kennung: HNSHA
Bezugssegment: -
Segmentversion: 1
Sender: Kunde/Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Sicherheitskontrollreferenz	DE	an	..14	M	1	<>0
3	Validierungsergebnis	DE	bin	..512	M	1	

◆ Erläuterungen

Nr. 2: Sicherheitskontrollreferenz

Stellt die Verbindung zwischen Signaturkopf und -abschluß sicher. Es enthält den gleichen Wert, wie das gleichnamige Feld im Signaturkopf.

Nr. 3: Validierungsergebnis

Enthält die elektronische Signatur.

◆ Beispiel

HNSHA:8:1+654321+@96@<Signatur>'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung	Stand: 02.02.1998	Seite: 37

VI.5.4 Verschlüsselungskopf

VI.5.4.1 Segmentbeschreibung

◆ Beschreibung

Der Verschlüsselungskopf enthält Informationen über die Art des Sicherheitsservice, die Verschlüsselungsfunktion und die zu verwendenden Chiffrierschlüssel.

Zum Abgleich mit den in den BPD definierten Verschlüsselungsverfahren DDV bzw. RDH wird das Feld „Bezeichner für Algorithmusparameter, Schlüssel“ herangezogen (vgl. Kap. VI.5.4.2).

◆ Format

Name: Verschlüsselungskopf
 Typ: Segment
 Segmentart: Administration
 Kennung: HNVSK
 Bezugssegment: -
 Segmentversion: 2
 Sender: Kunde/Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Sicherheitsfunktion, kodiert	DE	an	..3	M	1	4
3	Rolle des Sicherheitslieferanten, kodiert	DE	an	..3	M	1	1, 4
4	Sicherheitsidentifikation, Details	DEG			M	1	
5	Sicherheitsdatum und -uhrzeit	DEG			M	1	
6	Verschlüsselungsalgorithmus	DEG			M	1	
7	Schlüsselname	DEG			M	1	
8	Komprimierungsfunktion	DE	an	..3	M	1	0
9	Zertifikat	DEG			K	1	

◆ Erläuterungen

Nr. 2: Sicherheitsfunktion, kodiert

Spezifiziert die auf die Nachricht angewendete Sicherheitsfunktion.

Im Zusammenhang mit Verschlüsselung und Komprimierung ist momentan nur folgender Wert möglich:

- "4" für ENC, Encryption (Verschlüsselung und evtl. Komprimierung)

Nr. 3: Rolle des Sicherheitslieferanten, kodiert

Beschreibt das Verhältnis desjenigen, der die Sicherheit gewährleistet bezüglich der zu sichernden Nachricht.

Es sind folgende Werte möglich:

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 38	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung

- "1" für ISS, Herausgeber der chiffrierten Nachricht (Erfasser)
- "4" für WIT, der Unterzeichnete ist Zeuge, aber für den Inhalt der Nachricht nicht verantwortlich (Übermittler, welcher nicht Erfasser ist).

Nr. 4: Sicherheitsidentifikation, Details

Identifikation der im Sicherheitsprozeß involvierten Parteien. Dient zur Übermittlung der CID im DDV-Verfahren bzw. der Kundensystem-ID im RDH-Verfahren.

Details siehe VI.5.1.3

Nr. 5: Sicherheitsdatum und -uhrzeit

Zeitstempel, der anzeigt, wann die Sicherheitsfunktion angewendet wurde. Als Bedeutung wird „1“ eingestellt, da es sich um einen Sicherheitszeitstempel handelt.

Details siehe VI.5.1.2

Nr. 6: Verschlüsselungsalgorithmus

Enthält einen kryptographischen Algorithmus, seinen Operationsmodus, so wie dessen Einsatz, in diesem Fall den verschlüsselten Nachrichtenschlüssel und den Initialisierungsvektor.

Details siehe VI.5.4.2

Nr. 7: Schlüsselname

Enthält den verwendeten Schlüsselnamen, respektive die Referenz auf den Chiffrierschlüssel.

Details siehe VI.5.1.1

Nr. 8: Komprimierungsfunktion

Für die verschiedenen Komprimierungsverfahren sind folgende Werte vorgesehen:

- "0" für NULL, keine Kompression ⁷
- "1" für LZW, Lempel, Ziv, Welch
- "2" für COM, optimized LZW
- "3" für LZSS, Lempel, Ziv
- "4" für LZHuf, LZ + Huffman Coding
- "5" für ZIP, PKZIP
- "999" für ZZZ, gegenseitig vereinbart

Nr. 9: Zertifikat

Hier wird bei späterem Einsatz von Zertifizierungsinstanzen ein Zertifikat transparent eingestellt.

Details siehe VI.5.1.4

⁷ Z.Zt. wird nur der Wert „0“ für „keine Kompression“ unterstützt.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung	Stand: 02.02.1998	Seite: 39

◆ **Beispiel**

```
HNVSK:998:2+4+1+1::1+1:19960610:102044+2:2:13:@9
6@<chiffrierter Schlüssel>:6:1+280:10020030:1234
5:V:1:1+0'
```

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 40	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung

VI.5.4.2 Verschlüsselungsalgorithmus

◆ Beschreibung

Enthält einen kryptographischen Algorithmus, seinen Operationsmodus, so wie dessen Einsatz.

◆ Format

Name: Verschlüsselungsalgorithmus
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Verwendung des Verschlüsselungsalgorithmus, kodiert	GD	an	..3	M	1	2
2	Operationsmodus, kodiert	GD	an	..3	M	1	2
3	Verschlüsselungsalgorithmus, kodiert	GD	an	..3	M	1	13
4	Wert des Algorithmusparameters, Schlüssel	GD	bin	..512	M	1	
5	Bezeichner für Algorithmusparameter, Schlüssel	GD	an	..3	M	1	5,6
6	Bezeichner für Algorithmusparameter, IV	GD	an	..3	M	1	1
7	Wert des Algorithmusparameters, IV	GD	bin	..512	K	1	

◆ Erläuterungen

Nr. 1: Verwendung des Verschlüsselungsalgorithmus, kodiert

Spezifiziert die Verwendung des in Feld 2 identifizierten Algorithmus.

Im Zusammenhang mit der Verschlüsselung sind derzeit folgende Werte möglich:

- "2" für OSY, Owner Symmetric

Nr. 2: Operationsmodus, kodiert

Spezifiziert den verwendeten Operationsmodus:

- "2" für CBC, Cipher Block Chaining.

Nr. 3: Verschlüsselungsalgorithmus, kodiert

Spezifiziert den verwendeten Verschlüsselungsalgorithmus:

- "13" für 2-Key-Triple-DES

Nr. 4: Wert des Algorithmusparameters, Schlüssel

Dieser Algorithmusparameter enthält den verschlüsselten Nachrichtenschlüssel, welcher im Feld "Wert des Algorithmusparameters, Schlüssel" steht.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung	Stand: 02.02.1998	Seite: 41

Nr. 5: Bezeichner für Algorithmusparameter, Schlüssel

Das Feld enthält die genaue Eigenschaft für die beiden Verfahren DDV und RDH (Die Steuerung erfolgt in den BPD, vgl. Kapitel IV.4). Es werden in HBCI folgende Werte verwendet:

- „5“ für KYE, Symmetrischer Schlüssel, ver- bzw. entschlüsselt mit einem symmetrischen Schlüssel bei DDV (vgl. Kapitel VI.2.2.1).
- „6“ für KYP, Symmetrischer Schlüssel, verschlüsselt mit einem öffentlichen Schlüssel bei RDH.

Nr. 6: Bezeichner für Algorithmusparameter, IV

- "1" für IVC, Initialization value, cleartext

Nr. 7: Wert des Algorithmusparameters, IV

Es wird folgender Initialisierungswert als Default verwendet:

X'00 00 00 00 00 00 00 00'.

In einer zukünftigen Version kann dieses DE mit einem abweichenden Initialisierungswert belegt werden. Zur Zeit ist die Belegung nicht zulässig.

♦ Beispiel

2:2:13:@96@<chiffrierter Schlüssel>:6:1

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 42	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Formate für Signatur und Verschlüsselung

VI.5.5 Verschlüsselte Daten

◆ Beschreibung

Dieses Segment enthält die verschlüsselten (und komprimierten) Daten.

◆ Format

Name: Verschlüsselte Daten
 Typ: Segment
 Segmentart: Administration
 Kennung: HNVSD
 Bezugssegment: -
 Segmentversion: 1
 Sender: Kunde/Kreditinstitut

Nr.	Name	Typ	For- mat	Län- ge	Sta- tus	An- zahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Daten, verschlüsselt	DE	bin	..	M	1	

◆ Erläuterungen

Nr. 2: Daten, verschlüsselt

Enthält die verschlüsselten (und komprimierten) Daten.

◆ Beispiel

```
HNVSD:999:1+@348@<Daten, verschlüsselt>'
```


Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Key-Management	Stand: 02.02.1998	Seite: 43

VI.6 Key-Management

VI.6.1 Formate für Key-Management

Für die Schlüsseländerung, die Schlüsselverteilung sowie die Schlüsselsperrung sind die nachfolgenden Segmente vorgesehen. Diese dürfen nur im Rahmen der speziellen Key-Management-Nachrichten verwendet werden.

VI.6.1.1 Änderung eines öffentlichen Schlüssels

◆ Beschreibung

Dieses Segment enthält einen neuen öffentlichen Schlüssel des Kunden.

◆ Format

Name: Schlüsseländerung
Typ: Segment
Segmentart: Administration
Kennung: HKSAK
Bezugssegment: -
Segmentversion: 2
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Nachrichtenbeziehung, kodiert	DE	num	1	M	1	2
3	Bezeichner für Funktionstyp	DE	num	..3	M	1	112
4	Schlüsselname	DEG			M	1	
5	Öffentlicher Schlüssel	DEG			M	1	
6	Zertifikat	DEG			K	1	

◆ Erläuterungen

Nr. 2: Nachrichtenbeziehung, kodiert

Im Zusammenhang mit der Schlüsseländerung ist immer folgender Wert vorgesehen:

- "2" für 'Key-Management-Nachricht erwartet Antwort'

Nr. 3: Bezeichner für Funktionstyp

Im Zusammenhang mit der Schlüsseländerung ist folgender Wert vorgesehen:

- "112" für 'Certificate Replacement' (Ersatz des Zertifikats)

Nr. 4: Schlüsselname

Es ist der neue öffentliche Schlüssel des Kunden einzustellen. Als Schlüsselart darf nicht 'B' eingestellt werden, da in einem Auftragssegment nur ein Schlüssel übertragen werden kann.

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 44	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Key-Management

Details siehe VI.5.1.1

Nr. 5: Öffentlicher Schlüssel

Datenelementgruppe zur Aufnahme des neuen öffentlichen Schlüssels des Kunden.

Details siehe VI.5.1.5

Nr. 6: Zertifikat

Hier wird bei späterem Einsatz von Zertifizierungsinstanzen ein Zertifikat transparent eingestellt.

Details siehe VI.5.1.4

◆ Beispiel

```
HKSAK:8:2+2+112+280:10020030:12345:S:1:1+6:16:10
:@12@<Modulus>:12:@3@<Exponent>:13'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Key-Management	Stand: 02.02.1998	Seite: 45

VI.6.1.2 Anforderung eines öffentlichen Schlüssels

◆ Beschreibung

Dieses Segment enthält die Anfrage nach einem öffentlichen Schlüssel des Kreditinstituts. Das Segment wird entweder innerhalb der Dialoginitialisierung (vgl. Kapitel III.3.1) oder im Rahmen der erstmaligen Schlüsselanforderung (vgl. Kapitel VI.6.2.2) gesendet.

◆ Format

Name: Anforderung eines öffentlichen Schlüssels
Typ: Segment
Segmentart: Administration
Kennung: HKISA
Bezugssegment: -
Segmentversion: 2
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Nachrichtenbeziehung, kodiert	DE	num	1	M	1	2
3	Bezeichner für Funktionstyp	DE	num	..3	M	1	124
4	Schlüsselname	DEG			M	1	
5	Zertifikat	DEG			K	1	

◆ Erläuterungen

Nr. 2: Nachrichtenbeziehung, kodiert

Im Zusammenhang mit der Anfrage nach einem öffentlichen Schlüssel ist immer folgender Wert vorgesehen:

- "2" für 'Key-Management-Nachricht erwartet Antwort'

Nr. 3: Bezeichner für Funktionstyp

Im Zusammenhang mit der Anfrage für einen öffentlichen Schlüssel ist folgender Wert vorgesehen:

- "124" für 'Certificate Status Request'

Nr. 4: Schlüsselname

In den Schlüsselnamen ist die Schlüsselnummer und -version des Schlüssels einzustellen, den das Kundenprodukt als aktuellen öffentlichen Schlüssel des Kreditinstituts kennt. Falls dieser noch nicht vorliegt, ist in beide Felder der Wert „999“ einzustellen.

Details siehe VI.5.1.1

Nr. 5: Zertifikat

Hier wird bei späterem Einsatz von Zertifizierungsinstanzen ein Zertifikat transparent eingestellt.

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 46	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Key-Management

Details siehe VI.5.1.4

◆ **Beispiel**

HKISA:8:2+2+124+280:10020030:12345:S:1:1'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Key-Management	Stand: 02.02.1998	Seite: 47

VI.6.1.3 Übermittlung eines öffentlichen Schlüssels

◆ Beschreibung

Dieses Segment wird zum einen innerhalb der Dialoginitialisierungsantwort (vgl. Kapitel III.3.2) an den Kunden übertragen, falls sich der öffentliche Schlüssel des Kreditinstituts geändert hat. Es enthält dann jeweils einen öffentlichen Schlüssel des Kreditinstituts.

Zum anderen wird das Segment im Rahmen der erstmaligen Anforderung der öffentlichen Schlüssel des Kreditinstituts (vgl. Kapitel VI.6.2.2) benötigt.

◆ Format

Name: Übermittlung eines öffentlichen Schlüssels
Typ: Segment
Segmentart: Administration
Kennung: HIIISA
Bezugssegment: HKISA
Segmentversion: 2
Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Nachrichtenbeziehung, kodiert	DE	num	1	M	1	1
3	Austauschkontrollreferenz	DE	id	#	M	1	
4	Nachrichtenreferenznummer	DE	num	..4	M	1	>0
5	Bezeichner für Funktionstyp	DE	num	..3	M	1	224
6	Schlüsselname	DEG			M	1	
7	Öffentlicher Schlüssel	DEG			M	1	
8	Zertifikat	DEG			K	1	

◆ Erläuterungen

Nr. 2: Nachrichtenbeziehung, kodiert

Es ist folgender Wert vorgesehen:

- "1" für 'Key-Management-Nachricht ist Antwort'

Nr. 3: Austauschkontrollreferenz

Dialog-ID der Anfragenachricht des Kunden (vgl. Kapitel II.6.2).

Nr. 4: Nachrichtenreferenznummer

Nachrichtennummer der Anfragenachricht des Kunden (vgl. Kapitel II.6.2).

Nr. 5: Bezeichner für Funktionstyp

Es ist folgender Wert vorgesehen:

- "224" für 'Certificate Status Notice'

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 48	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Key-Management

Nr. 6: Schlüsselname

Der zurückgemeldete Schlüsselname enthält insbesondere die zugehörige Schlüssel- und Versionsnummer, die das Kundenprodukt für die Referenzierung des in der DEG „Öffentlicher Schlüssel“ übertragenen neuen öffentlichen Schlüssels verwendet.

Details siehe VI.5.1.1

Nr. 7: Öffentlicher Schlüssel

Diese Datenelementgruppe enthält den neuen öffentlichen Schlüssel des Kreditinstitutes.

Details siehe VI.5.1.5

Nr. 8: Zertifikat

Hier wird bei späterem Einsatz von Zertifizierungsinstanzen ein Zertifikat transparent eingestellt.

Details siehe VI.5.1.4

◆ Beispiel

```
HIISA:8:2:8+1+4711+1+224+280:10020030:12345:S:1:
1+6:16:10:@12@<Modulus>:12:@3@<Exponent>:13'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Key-Management	Stand: 02.02.1998	Seite: 49

VI.6.1.4 Schlüsselsperrung

◆ Beschreibung

Dieses Segment enthält die Anforderung für das Sperren eines Schlüssels.

◆ Format

Name: Schlüsselsperrung
 Typ: Segment
 Segmentart: Administration
 Kennung: HKSSP
 Bezugssegment: -
 Segmentversion: 2
 Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Nachrichtenbeziehung, kodiert	DE	num	1	M	1	2
3	Bezeichner für Funktionstyp	DE	num	..3	M	1	130
4	Schlüsselname	DEG			M	1	
5	Sperrenkennzeichen	DE	an	..3	M	1	1, 501, 999
6	Sicherheitsdatum und -uhrzeit	DEG			K	1	
7	Zertifikat	DEG			K	1	

◆ Erläuterungen

Nr. 2: Nachrichtenbeziehung, kodiert

Im Zusammenhang mit der Schlüsselsperrung ist folgender Wert vorgesehen:

- "2" für 'Key-Management-Nachricht erwartet Antwort'

Nr. 3: Bezeichner für Funktionstyp

Im Zusammenhang mit der Schlüsselsperrung ist folgender Wert vorgesehen:

- "130" für 'Certificate Revocation' (Zertifikatswiderruf)

Nr. 4: Schlüsselname

Es sind die Identifikationsmerkmale des zu sperrenden Signierschlüssels einzustellen, unabhängig davon, daß grundsätzlich immer sowohl Signier- als auch Chiffrierschlüssel gesperrt werden (s. Kap. VI.6.2.4).

Format siehe VI.5.1.1

Nr. 5: Sperrenkennzeichen

Enthält folgende Werte als Begründung für die Sperrung:

- "1" für 'Schlüssel des Zertifikatseigentümers kompromittiert'

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 50	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Key-Management

- "501" für 'Zertifikat ungültig wegen Verdacht auf Kompromittierung'
- "999" für 'gesperrt aus sonstigen Gründen'

Nr. 6: Sicherheitsdatum und -uhrzeit

Enthält optional Datum und Uhrzeit, ab welcher der Schlüssel nicht mehr gültig ist. Als Bedeutung wird „6“ eingestellt, da Datum und Zeit das Ende der Gültigkeit anzeigen.

Details siehe VI.5.1.2



Es ist zu beachten, daß eine terminierte Sperre nicht von allen Kreditinstituten unterstützt wird. Das Kundenprodukt sollte den Kunden auf diesen Sachverhalt hinweisen.

Nr. 7: Zertifikat

Hier wird bei späterem Einsatz von Zertifizierungsinstanzen ein Zertifikat transparent eingestellt.

Details siehe VI.5.1.4

◆ Beispiel

```
HKSSP:8:2+2+130+280:10020030:12345:S:1:1+501'
```


Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Key-Management	Stand: 02.02.1998	Seite: 51

VI.6.1.5 Bestätigung der Schlüsselsperrung

◆ Beschreibung

Dieses Segment enthält die Bestätigung für eine Schlüsselsperrung.

◆ Format

Name: Bestätigung der Schlüsselsperrung
 Typ: Segment
 Segmentart: Administration
 Kennung: HISSP
 Bezugssegment: HKSSP
 Segmentversion: 2
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Nachrichtenbeziehung, kodiert	DE	num	1	M	1	1
3	Austauschkontrollreferenz	DE	id	#	M	1	
4	Nachrichtenreferenznummer	DE	num	..4	M	1	>0
5	Bezeichner für Funktionstyp	DE	num	..3	M	1	231
6	Schlüsselname	DEG			M	1	
7	Sperrenkennzeichen	DE	an	..3	M	1	1, 501, 999
8	Sicherheitsdatum und -uhrzeit	DEG			M	1	
9	Zertifikat	DEG			K	1	

◆ Erläuterungen

Nr. 2: Nachrichtenbeziehung, kodiert

Im Zusammenhang mit der Schlüsselsperrung ist folgender Wert vorgesehen:

- "1" für 'Key-Management-Nachricht ist Antwort'

Nr. 3: Austauschkontrollreferenz

Dialog-ID der Sperrnachricht des Kunden (vgl. Kapitel II.6.2).

Nr. 4: Nachrichtenreferenznummer

Nachrichtennummer der Sperrenanforderung des Kunden (vgl. Kapitel II.6.2).

Nr. 5: Bezeichner für Funktionstyp

Im Zusammenhang mit der Schlüsselsperrung ist folgender Wert vorgesehen:

- "231" für 'Revocation Confirmation' (Bestätigung des Zertifikatswiderrufs)

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 52	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Key-Management

Nr. 6: Schlüsselname

Es sind die Identifikationsmerkmale des gesperrten Signierschlüssels einzustellen, unabhängig davon, daß grundsätzlich immer sowohl Signier- als auch Chiffrierschlüssel gesperrt werden (s. Kap. VI.6.2.4).

Format siehe VI.5.1.1

Nr. 7: Sperrenkennzeichen

Kann folgende Werte enthalten:

- "1" für 'Schlüssel des Zertifikatseigentümers kompromittiert'
- "501" für 'Zertifikat ungültig wegen Verdacht auf Kompromittierung'
- "999" für 'gesperrt aus sonstigen Gründen'

Nr. 8: Sicherheitsdatum und -uhrzeit

Enthält Datum und Uhrzeit, ab welchem das Zertifikat nicht mehr gültig sein soll. Als Bedeutung wird „6“ eingestellt, da Datum und Zeit das Ende der Gültigkeit anzeigen.

Details siehe VI.5.1.2

Nr. 9: Zertifikat

Hier wird bei späterem Einsatz von Zertifizierungsinstanzen vom Kreditinstitut ein Zertifikat transparent eingestellt, um die Sperrung zu bestätigen.

Details siehe VI.5.1.4

◆ Beispiel

```
HISSP:8:2:8+1+4711+2+231+280:10020030:12345:S:1:
1+501+6:19960611:111734'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Key-Management	Stand: 02.02.1998	Seite: 53

VI.6.2 Key-Management-Nachrichten

Aufträge des Key-Managements dürfen nur in den folgenden separaten Nachrichten übertragen werden.

Hiervon abweichend wird der Auftrag „Anforderung eines öffentlichen Schlüssels des Kreditinstituts“ nicht als eigene Nachricht, sondern innerhalb der Dialoginitialisierung übertragen.

Die Nachrichten für das Key-Management müssen zum Teil kryptographisch geschützt werden. Alternativ können auch Offline-Sicherungsverfahren (z.B. Brief) zum Einsatz kommen (vgl. Kapitel VI.3.1.3).

Es sind folgende Key-Management-Nachrichten vorgesehen:

- Änderung eines öffentlichen Schlüssels des Kunden
- Erstmalige Anforderung der Schlüssel des Kreditinstituts
- Erstmalige Übermittlung der Schlüssel des Kunden
- Schlüsselsperrung den Kunden

Mit Ausnahme der Sperrnachricht sind alle Key-Management-Nachrichten nur bei Einsatz des RDH-Verfahrens möglich.

VI.6.2.1 Änderung eines öffentlichen Schlüssels des Kunden

Realisierung Bank: verpflichtend

Realisierung Kunde: verpflichtend

a) Kundennachricht

◆ Beschreibung

Diese Nachricht ist nur bei Verwendung des RDH-Verfahrens möglich. Der Nachricht muß eine Dialoginitialisierung vorausgehen. Der Auftrag muß mit dem alten Signierschlüssel signiert werden.

Zum Verfahren s. Kap. VI.3.1.3.3.

◆ Format

Name: Änderung eines öffentlichen Schlüssels des Kunden

Typ: Nachricht

Sender: Kunde

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	M	1	s. Kap. VI.5.2
3	Schlüsseländerung	SEG	HKSAK	M	1-2	s. Kap. VI.6.1.1
4	Signaturabschluß	SEG	HNSHA	M	1	s. Kap. VI.5.3
5	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 54	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Key-Management

◆ Erläuterungen

Nr. 3: Schlüsseländerung

Der Kunde stellt entweder seinen neuen öffentlichen Signierschlüssel, seinen neuen öffentlichen Chiffrierschlüssel oder beide Schlüssel ein.

b) Kreditinstitutsnachricht

◆ Format

Name: Kreditinstitutsnachricht allgemein
Typ: Nachricht
Format: s. Kap. II.8.1

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel
0020	Öffentlicher Schlüssel wurde geändert
9010	Schlüsseländerung zur Zeit nicht möglich
9010	Sicherheitsverfahren unterstützt keine öffentlichen Schlüssel
9210	Eingereichter Schlüssel ist mit dem aktuellen Schlüssel identisch

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Key-Management	Stand: 02.02.1998	Seite: 55

VI.6.2.2 Erstmalige Anforderung der Schlüssel des Kreditinstituts

Mit Hilfe dieser Nachricht fordert der Kunde erstmalig den öffentlichen Signier- und Chiffrierschlüssel des Kreditinstituts an. Gleichzeitig erhält er die aktuellen Bankparameterdaten, die er benötigt, um die unterstützten Verschlüsselungsverfahren des Kreditinstituts in Erfahrung zu bringen. Mit Hilfe dieser Informationen wird der Kunde in die Lage versetzt, beliebige Nachrichten zu verschlüsseln.

Realisierung Bank: optional

Realisierung Kunde: verpflichtend

a) Kundennachricht

◆ Beschreibung

Diese Nachricht wird an Stelle einer Dialoginitialisierung gesendet. Es dürfen keine Auftragsnachrichten folgen. Der Dialog ist vom Kunden nach Erhalt der Antwortnachricht mit einer Dialogendenachricht zu beenden. Die Nachricht wird weder signiert noch verschlüsselt.

◆ Format

Name: Erstmalige Anforderung der Schlüssel des Kreditinstituts
Typ: Nachricht
Sender: Kunde

Nr.	Name	Typ	Ken-nung	Sta-tus	An-zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Identifikation	SEG	HKIDN	M	1	s. Kap. III.3.1.2
3	Verarbeitungsvorbereitung	SEG	HKVVB	M	1	s. Kap. III.3.1.3
4	Anforderung eines öffentlichen Schlüssels	SEG	HKISA	M	2	s. Kap. VI.6.1.2
5	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

◆ Erläuterungen

Nr. 2: Identifikation

Die Datenelemente des Segments sind wie beim anonymen Zugang zu belegen (s. Kap. III.5).

Nr. 3: Verarbeitungsvorbereitung

Mit diesem Segment fordert der Kunde die Bankparameterdaten an.

Nr. 4: Anforderung eines öffentlichen Schlüssels

Mit diesen beiden Segmenten fordert der Kunde jeweils den öffentlichen Signierschlüssel und den öffentlichen Chiffrierschlüssel des Kreditinstituts an. Es sind stets beide Schlüssel anzufordern, auch wenn das Kreditinstitut nicht signiert.

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 56	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Key-Management

b) Kreditinstitutsnachricht

◆ Format

Name: Erstmalige Übermittlung der Schlüssel des Kreditinstituts
Typ: Nachricht
Sender: Kreditinstitut

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	K	0-1	s. Kap. VI.5.2
3	Rückmeldungen zur Ge- samtnachricht	SEG	HIRMG	M	1	s. Kap. II.8.2
4	Rückmeldungen zu Seg- menten	SEG	HIRMS	K	0-n	s. Kap. II.8.3
5	Bankparameterdaten	SF	#	K	1	s. Kap. III.3.2.2
6	Übermittlung eines öffent- lichen Schlüssels	SEG	HIISA	M	1-2	s. Kap. VI.6.1.3
7	Signaturabschluß	SEG	HNSHA	K	0-1	s. Kap. VI.5.3
8	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

◆ Erläuterungen

Nr. 2: Signaturkopf

Falls das Kreditinstitut einen Signierschlüssel besitzt, d.h. seine Nachrichten grundsätzlich signiert, hat es auch diese Nachricht zu signieren, um die Authentizität des Chiffrierschlüssels zu sichern (s.u.).

Nr. 6: Übermittlung eines öffentlichen Schlüssels

In diesen beiden Segmenten werden dem Kunden die öffentlichen Schlüssel des Kreditinstituts mitgeteilt.

Falls das Kreditinstitut seine Nachrichten nicht signiert, erhält der Kunde nur den öffentlichen Chiffrierschlüssel zurückgemeldet. Auf die Anforderung des Signierschlüssels erhält er einen entsprechenden Rückmeldungscode, der ihm anzeigt, daß das Kreditinstitut seine Nachrichten nicht signiert. Da die Authentizität des Chiffrierschlüssels nicht gesichert ist, muß diese Nachricht durch einen Ini-Brief an den Kunden mit dem Hashwert des Chiffrierschlüssels begleitet werden (s. Kap. VI.3.1.3.2).

Falls das Kreditinstitut seine Nachrichten signiert, erhält der Kunde sowohl den öffentlichen Chiffrier- als auch Signierschlüssel zurückgemeldet. Die Authentizität des Chiffrierschlüssels ist dabei durch die Signatur gesichert. Die Authentizität des Signierschlüssels ist jedoch nicht gesichert, da das Kundensystem die Echtheit der Signatur nicht prüfen kann. Daher muß in diesem Fall die Nachricht durch einen Ini-Brief mit dem Hashwert des Signierschlüssels begleitet werden.

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel
0020	Auftrag ausgeführt
9010	Kein Schlüssel verfügbar, da Kreditinstitutsnachrichten nicht signiert werden

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Key-Management	Stand: 02.02.1998	Seite: 57

VI.6.2.3 Erstmalige Übermittlung der Schlüssel des Kunden

Mit Hilfe dieser Nachricht übermittelt der Kunde erstmalig seinen öffentlichen Signier- und Chiffrierschlüssel an das Kreditinstitut („Erstinitialisierungsnachricht“).

Da der Absender des öffentlichen Schlüssels den Beweis erbringen muß, daß er auch im Besitz des zugehörigen privaten Schlüssels ist, muß die Nachricht des Kunden signiert sein.



Das Kreditinstitut darf eine Nachricht nicht ablehnen, nur weil für den Kunden noch kein öffentlicher Schlüssel in der Schlüsselverwaltung existiert. Falls die normale Signaturprüfung aus diesem Grund negativ verläuft, muß zunächst geprüft werden, ob es sich um eine Erstinitialisierung handelt. In diesem Fall ist der öffentliche Schlüssel aus der Erstinitialisierungsnachricht zu extrahieren und die Signaturprüfung auf der Basis dieses Schlüssels erneut vorzunehmen.

Die Erstinitialisierungsnachricht des Kunden ist zu verschlüsseln, da die darin enthaltenen benutzerbezogenen Daten (Kunden-ID, Benutzerkennung) als vertraulich einzustufen sind. Dies erfordert, daß sich der öffentliche Chiffrierschlüssel des Kreditinstituts schon vor dem Senden der Erstinitialisierung im Besitz des Kunden befinden muß. Ferner muß dem Kunden das Verschlüsselungsverfahren bekannt sein, das ihm in den Bankparameterdaten mitgeteilt wird. Um dem Kunden diese Daten vorab zukommen zu lassen bieten sich folgende Lösungen an:

- Das Kreditinstitut sendet dem Kunden eine Diskette zu, die die Schlüssel und die aktuelle BPD enthält, wie in VI.3.1.3.2 beschrieben.
- Der Kunde sendet die Key-Management-Nachricht „Erstmalige Anforderung der Schlüssel des Kreditinstituts“ (s. Kap. VI.6.2.2). Diese Nachricht wird begleitet von einem Ini-Brief.



Um die wiederholte Ausführung unberechtigter Initialisierungsversuche zu verhindern, sind kreditinstitutsseitig folgende Vorkehrungen zu treffen:

- Die Benutzerkennung sollte bei Verwendung des RDH-Verfahrens nicht durch benutzerindividuelle Merkmale (z.B. Kontonummer) hergeleitet werden können.
- Eine weitere Erstinitialisierung unter derselben Benutzerkennung und Kunden-ID hat zur Ablehnung der Nachricht zu führen.

Realisierung Bank: verpflichtend

Realisierung Kunde: verpflichtend

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 58	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Key-Management

a) Kundennachricht

◆ Beschreibung

Diese Nachricht wird an Stelle einer Dialoginitialisierung gesendet. Es dürfen keine Auftragsnachrichten folgen. Der Dialog ist vom Kunden nach Erhalt der Antwortnachricht mit einer Dialogendenachricht zu beenden. Die Nachricht muß signiert und verschlüsselt werden.

◆ Format

Name: Erstmalige Übermittlung der Schlüssel des Kunden
Typ: Nachricht
Sender: Kunde

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	M	1	s. Kap. VI.5.2
3	Identifikation	SEG	HKIDN	M	1	s. Kap. III.3.1.2
4	Schlüsseländerung	SEG	HKSAK	M	2	s. Kap. VI.6.1.1
5	Signaturabschluß	SEG	HNSHA	M	1	s. Kap. VI.5.3
6	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

◆ Erläuterungen

Nr. 3: Identifikation

Der Benutzer hat die ihm zur Initialisierung mitgeteilten Daten einzustellen. Da zu diesem Zeitpunkt noch keine Synchronisierung durchgeführt wurde, ist als Kundensystem-ID der Wert '0' einzustellen.

Nr. 4: **Schlüsseländerung**

Der Kunde stellt seinen öffentlichen Signier- und Chiffrierschlüssel ein.

Die Authentizität des Chiffrierschlüssels ist dabei durch die Signatur gesichert. Die Authentizität des Signierschlüssels ist jedoch nicht gesichert, da das Kreditinstitut die Echtheit der Signatur nicht prüfen kann. Daher muß die Nachricht durch einen Ini-Brief an das Kreditinstitut mit dem Hashwert des Signierschlüssels begleitet werden (s. Kap. VI.3.1.3.2).

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Key-Management	Stand: 02.02.1998	Seite: 59

b) Kreditinstitutsnachricht

◆ Beschreibung



Die Ablehnung der Erstinitialisierungsnachricht darf aus sicherheitstechnischen Aspekten im Rahmen der Rückmeldungs_codes nicht inhaltlich begründet werden. Fehlermeldungen, die sich auf den syntaktischen Aufbau der Nachricht bzw. der Segmente beziehen, sind hiervon unberührt.

◆ Format

Name: Kreditinstitutsnachricht allgemein
Typ: Nachricht
Format: s. Kap. II.8.1

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

◆ Ausgewählte Beispiele für Rückmeldungs_codes

Code	Beispiel
0010	Öffentlicher Schlüssel wurde entgegengenommen
0020	Öffentlicher Schlüssel wurde freigeschaltet
0020	Kunde wurde freigeschaltet
9010	Auftrag abgelehnt

Kapitel: VI	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 60	Stand: 02.02.1998	Kapitel: Sicherheit Abschnitt: Key-Management

VI.6.2.4 Schlüsselsperrung durch den Kunden

Diese Nachricht beschreibt die Anforderung zum Sperren der Schlüssels durch den Kunden und die Bestätigung der Schlüsselsperrung durch das Kreditinstitut (vgl. Kapitel VI.3.3).

Realisierung Bank: verpflichtend

Realisierung Kunde: verpflichtend

a) Kundennachricht

◆ Beschreibung

Es werden immer beide Schlüssel (Signier- und Chiffrierschlüssel) gesperrt. Eine selektive Schlüsselsperrung ist gegenwärtig nicht zulässig.

Der Nachricht muß eine Dialoginitialisierung vorausgehen. Die Nachricht muß bei Kompromittierung signiert sein. Es liegt in der Entscheidung des Kreditinstituts, ob es auch nicht signierte (anonyme) Schlüsselsperrungen erlaubt (z.B. bei Verlust des Sicherheitsmediums). Die Steuerung erfolgt in den Userparameterdaten über das Feld „Anzahl benötigter Signaturen“.

Bei Verlust des Sicherheitsmediums liegen dem Benutzer u.U. die zur Durchführung der Sperrung erforderlichen Daten (Schlüsselnummer und -version) nicht vor. In diesem Fall ist zur Referenzierung auf den aktuellen Schlüssel jeweils der Wert '999' einzustellen. Es ist daher darauf zu achten, daß dieser Wert reserviert ist und nicht im Rahmen der Versionszählung belegt wird.



Falls das Kreditinstitut unsignierte Sperrungen zuläßt, muß dem Benutzer darüber hinaus explizit seine Benutzerkennung mitgeteilt werden. Beim RDH-Verfahren erfolgt dies im Rahmen des Ini-Briefs. Beim DDV-Verfahren kann diese dem Benutzer bei der Aushändigung der Chipkarte mitgeteilt werden.

Beim RDH-Verfahren muß der Kunde nach einer Schlüsselsperrung zur Entsperrung eine erneute Erstinitialisierung durchführen.

◆ Format

Name: Sperrung eines Schlüssels durch den Kunden

Typ: Nachricht

Sender: Kunde

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	K	0-1	s. Kap. VI.5.2
3	Schlüsselsperrung	SEG	HKSSP	M	1	s. Kap. VI.6.1.4
4	Signaturabschluß	SEG	HNSHA	K	0-1	s. Kap. VI.5.3
5	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VI
Kapitel: Sicherheit Abschnitt: Key-Management	Stand: 02.02.1998	Seite: 61

◆ Erläuterungen

Nr. 3: Schlüsselsperrung

Dieses Segment enthält die Anforderung für die Schlüsselsperrung.

Eine selektive Schlüsselsperrung ist gegenwärtig nicht zulässig, d.h. es werden immer beide Schlüssel (Signier- und Chiffrierschlüssel) gleichzeitig gesperrt. In der DEG „Schlüsselname“ sind die Merkmale des Signierschlüssels einzustellen (s. Kap. VI.6.1.4).

b) Kreditinstitutsnachricht

◆ Format

Name: Bestätigung der Schlüsselsperrung durch das Kreditinstitut
Typ: Nachricht
Sender: Kreditinstitut

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	K	0-1	s. Kap. VI.5.2
3	Rückmeldungen zur Gesamtnachricht	SEG	HIRMG	M	1	s. Kap. II.8.2
4	Rückmeldungen zu Segmenten	SEG	HIRMS	K	0-n	s. Kap. II.8.3
5	Bestätigung der Schlüsselsperrung	SEG	HISSP	M	1	s. Kap. VI.6.1.5
6	Signaturabschluß	SEG	HNSHA	K	0-1	s. Kap. VI.5.3
7	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel
0020	Schlüssel wurde erfolgreich gesperrt
9010	Schlüssel ist bereits gesperrt
9010	Terminierte Sperren werden nicht unterstützt
9210	Unbekanntes Sperrenkennzeichen
9210	Sperrdatum liegt zu weit in der Zukunft

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 2	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Inhaltsverzeichnis

VII.6 Karten, Schecks und Formulare 109

VII.6.1 Bestellung.....	109
VII.6.1.1 Vordruckbestellung.....	109

VII.7 Informationen 113

VII.7.1 Freitextmeldungen.....	113
VII.7.1.1 Kundenmeldung.....	113
VII.7.1.2 Gastmeldung.....	116
VII.7.2 Formatierte Meldungen.....	118
VII.7.2.1 Kreditinstitutsangebote abholen.....	118
VII.7.2.2 Informationsbestellung	121
VII.7.2.3 Terminvereinbarung	123

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 3

VII.1 Zahlungsverkehr Inland

Generell wird für den Inlandszahlungsverkehr der DTAUS-Zeichensatz zugrundegelegt, damit die Aufträge ohne Zeichenkonvertierung in die DTAUS-Verarbeitung übernommen werden können.



Falls im Kundenprodukt für die Dateneingabe ein nachempfunder Zahlungsverkehrsvordruck verwendet wird, so hat sich die optische Gestaltung der Bildschirmmaske nach den „Richtlinien für einheitliche Zahlungsverkehrsvordrucke“ in der jeweils aktuellen Fassung zu richten.¹



Die meisten Kreditinstitute nutzen bei der Vergabe von Kontonummern Prüzzifferverfahren, die es vermeiden sollen, daß Zahlendreher und andere Fehler in der Kontonummernangabe bei Zahlungsaufträgen zu Fehlleitungen führen.

Die Deutsche Bundesbank hat hierzu eine Übersicht der im deutschen Kreditgewerbe verwendeten Prüzzifferverfahren erstellt und veröffentlicht regelmäßig in einem Bankleitzahl-Magnetband, welche Verfahren von welchen Kreditinstituten eingesetzt werden. Die korrekte Angabe der Kontonummer des Zahlungsempfängers/Zahlungspflichtigen sollte deshalb vom Kundenprodukt durch eine gesonderte Prüfroutine unterstützt werden. Falls diese Prüfung fehlschlägt, sollte das Kundenprodukt den Kunden auffordern, die eingegebene Kontonummer zu korrigieren. Bei erneutem Fehlschlagen der Prüzziffernkontrolle kann der Zahlungsauftrag dennoch an das Kreditinstitut übermittelt werden.

¹ Seit dem 1. Juni 1997 gelten aktualisierte Richtlinien, die insbesondere die Änderungen bzgl. des Euro beinhalten.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 4	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

VII.1.1 Einzelaufträge

Der Inlandszahlungsverkehr beruht weitgehend auf dem DTAUS-Verfahren. Für Einzelaufträge ist hiervon abweichend der folgende Segmentaufbau vorgesehen, da der DTA von seinem Aufbau her nicht auf Einzelaufträge zugeschnitten ist:

◆ Format

Name: Einzelauftrag Inlandszahlungsverkehr
Typ: Format

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kontoverbindung Auftraggeber	DEG	kto	#	M	1	
3	Kontoverbindung Empfänger/Zahlungspflichtiger	DEG	kto	#	M	1	
4	Name Empfänger/Zahlungspflichtiger 1	DE	an	..27	M	1	
5	Name Empfänger/Zahlungspflichtiger 2	DE	an	..27	K	1	
6	Betrag	DEG	btg	#	M	1	
7	Textschlüssel	DE	dig	2	M	1	
8	Textschüsselergänzung	DE	dig	3	K	1	
9	Verwendungszweck	DEG			K	1	
10	Ausführungsdatum	DE	dat	#	K	1	
11	Auftragsidentifikation	DE	an	..99	K	1	

◆ Erläuterungen

Nr. 2: Kontoverbindung Auftraggeber

Bei Überweisungen ist diejenige Kontoverbindung des Kunden einzustellen, von dem die Überweisung erfolgen soll. Bei Lastschriften ist die Kontoverbindung des Kunden einzustellen, dem die Lastschrift gutgeschrieben werden soll.

Nr. 3: Kontoverbindung Empfänger/Zahlungspflichtiger

Bei Überweisungen ist die Kontoverbindung des Überweisungsempfängers, bei Lastschriften die Kontoverbindung des Zahlungspflichtigen einzustellen. Diese muß einem deutschen Kreditinstitut zugeordnet sein.

Nr. 4: Name Empfänger/Zahlungspflichtiger 1

Bei Überweisungen ist der Name des Überweisungsempfängers, bei Lastschriften der Name des Zahlungspflichtigen einzustellen. Es ist der DTAUS0-Zeichensatz zu verwenden.

Nr. 5: Name Empfänger/Zahlungspflichtiger 2

Dieses Feld kann zusätzlich für den Name des Überweisungsempfängers bzw. Zahlungspflichtigen genutzt werden. Die Belegung sollte jedoch möglichst unterbleiben. Es ist der DTAUS0-Zeichensatz zu verwenden.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 5

Nr. 6: Betrag

Es ist der Betrag der Überweisung bzw. Lastschrift einzustellen. Dieser darf nicht 0 sein.

Nr. 7: Textschlüssel

Die vom Kreditinstitut unterstützten Textschlüssel werden dem Kundenprodukt in den Bankparameterdaten mitgeteilt.

Nr. 8: Textschlüsselergänzung

Wahlweise kann hier eine zum jeweiligen Textschlüssel korrespondierende Ergänzung eingestellt werden.

Nr. 9: Verwendungszweck

Die maximale Anzahl der Verwendungszweckzeilen ergibt sich aus den BPD. Es ist der DTAUS0-Zeichensatz zu verwenden. Die Daten dürfen nicht um führende oder nachfolgende Leerzeichen gekürzt werden.

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Verwendungszweckzeile	GD	an	..27	K	0..n	



Das Kundenprodukt hat bei der Darstellung des Verwendungszwecks die durch das Format vorgegebene Zeilenstruktur beizubehalten.

Nr. 10: Ausführungsdatum

Bei terminierten Überweisungen und Daueraufträgen ist das Ausführungsdatum des Auftrags einzustellen.

Nr. 11: Auftragsidentifikation

Eindeutiges Identifikationsmerkmal eines Auftrages. Die Auftragsidentifikation wird z.B. bei terminierten Überweisungen und Daueraufträgen benötigt, um Änderungen im Bestand vornehmen zu können.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 6	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

VII.1.1.1 Einzelüberweisung

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Einzelüberweisung
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKUEB
Bezugssegment: -
Segmentversion: 2
Sender: Kunde
Format: Einzelauftrag Inlandszahlungsverkehr

◆ Besondere Belegungsrichtlinien

Nr. 10: Ausführungsdatum

Die Belegung ist nicht zugelassen.

Nr. 11: Auftragsidentifikation

Die Belegung ist nicht zugelassen.

◆ Beispiel

```
HKUEB:4:2+1234567:280:10020030+7654321:280:20030
040+MEIER FRANZ++1000,:DEM+51+000+RE-NR.1234:KD-
NR.9876'
```

b) Kreditinstitutsrückmeldung

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 7

♦ Ausgewählte Beispiele für Rückmeldungs-codes

Code	Beispiel für Rückmeldungstext
0010	Auftrag zur Ausführung vorgemerkt
3020	Bankleitzahl veraltet. Die neue BLZ lautet
9150	Ausführungsdatum darf nicht belegt werden
9150	Identifikationsnr. darf nicht belegt werden
9210	Betrag zu groß für Überweisung
9210	Betrag muß größer als 0 sein
9210	Empfänger-Kontonummer existiert nicht
9210	Keine Berechtigung für dieses Konto
9210	Falscher Textschlüssel
9210	Keine gültige Kontoverbindung des Kunden
9210	BLZ existiert nicht
9230	Unzureichendes Guthaben des Kontos

c) Bankparameterdaten

♦ Format

Name: Einzelüberweisung Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIUEBS
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

♦ Erläuterungen

Nr. 4: Parameter

Name: Parameter Einzelüberweisung/-lastschrift
 Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Maximale Anzahl Verwendungszweckzeilen	GD	num	..2	M	1	
2	Textschlüssel	GD	dig	2	M	1..n	

Nr. 1: Maximale Anzahl Verwendungszweckzeilen

Es ist die maximale Anzahl der Verwendungszweckzeilen einzustellen, die der Kunde im Rahmen einer Einzelüberweisung belegen darf. Diese Anzahl hat sich an den DTA-Richtlinien zu orientieren (z.Zt. 0-14).

Nr. 2: Textschlüssel

Einzustellen sind die vom Kreditinstitut unterstützten Textschlüssel.² Hierzu gehört mindestens der Textschlüssel 51 („Überweisungsgutschrift“). Weiter-

² Ein Verzeichnis aller grundsätzlich für die Belegung durch den Kunden erlaubten Textschlüssel und Textschlüsselergänzungen befindet sich in der Anlage zum DTAUS-Format (Kap. VIII.9.1).

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 8	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

hin sind gemäß den Vorgaben für die Sonderformen der Überweisung (vgl. Kap. VII.1.1.2) auch die Textschlüssel 67 und 69 Pflicht.



Die Einstellung zulässiger Textschlüssel erfolgt nicht kunden-, sondern kreditinstitutsbezogen. Daher kann im Einzelfall ein Auftrag abgelehnt werden, da ein nicht erlaubter Textschlüssel eingereicht wurde, obwohl dieser laut BPD zulässig ist.

Beispiel: Kreditinstitutsseitig werden Lohn- und Gehaltsüberweisungen (Textschlüssel 53) zugelassen, diese Möglichkeit soll jedoch nicht für Privatkunden angeboten werden.

◆ Beispiel

HIUEBS:6:2:5+1+2+14:51:53:54:67:69'



Umbuchungen, d.h. Überweisungen auf eigene Konten, werden bei der Übertragung nicht gesondert gekennzeichnet, so daß vom Kreditinstitut der Wunsch des Kunden, eine Umbuchung durchzuführen, erkennbar wäre. Die Prüfung, ob die Voraussetzungen für eine Umbuchung gegeben sind, hat in jedem Fall durch das Kreditinstitut zu erfolgen. Daher sollte eine Umbuchung im Kundenprodukt nicht durch eine gesonderte Eingabemaske unterstützt werden, um nicht beim Kunden eine entsprechende Erwartungshaltung zu erzeugen.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 9

VII.1.1.2 Sonderformen der Überweisung

Spendenzahlungen und Überweisungen mit prüfziffergesicherten Verwendungszweckangaben sind Sonderformen, die einer gesonderten Behandlung bedürfen.³



Um hierbei Schwierigkeiten im Zahlungsverkehr zu vermeiden, sollten Hersteller von Kundenprodukten für diese Sonderformen gesonderte Eingabeformulare bzw. Eingabehinweise für den Kunden vorsehen, damit spezifische Angaben in der erforderlichen Weise eingetragen werden.

VII.1.1.2.1 Spendenzahlung

◆ Beschreibung

Bei Spendenzahlungen ist neben den übrigen Überweisungsdaten die Angabe des Absenders erforderlich, damit die empfangende Organisation dem Zahler eine Spendenquittung zukommen lassen kann.



Die Spendenüberweisung sollte vom Kundenprodukt durch eine gesonderte Eingabemaske unterstützt werden.⁴

Falls das Kundenprodukt eine Plausibilitätskontrolle der Empfängerkontonummer und Empfängerbankleitzahl durchführt, sollte diese bei Spendenüberweisungen nicht angewendet werden.

Realisierung Bank: verpflichtend, falls auch Einzelüberweisung angeboten wird, sonst optional

Realisierung Kunde: verpflichtend, falls auch Einzelüberweisung angeboten wird, sonst optional

◆ Format

Name: Spendenzahlung
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKUEB
Bezugssegment: -
Segmentversion: 2
Sender: Kunde
Format: Einzelauftrag Inlandszahlungsverkehr

³ Einzelheiten sind beschrieben in den „Richtlinien für einheitliche Zahlungsverkehrsvordrucke und Merkblätter für neutrale Zahlungsverkehrsvordrucke“.

⁴ Zur optischen Gestaltung s. Abb. 16 in „Richtlinien für einheitliche Zahlungsverkehrsvordrucke und Merkblätter für neutrale Zahlungsverkehrsvordrucke“.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 10	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

◆ Belegungsrichtlinien

Nr. 7: Textschlüssel

Es muß der Wert '69' eingestellt werden.

Nr. 9: Verwendungszweck

Es ist die Spenderadresse anzugeben.



Die Spenderadresse wird im Kundenprodukt in drei Verwendungszweckzeilen erfaßt⁵ (Hierzu müssen vom Kreditinstitut in den BPD mindestens drei Verwendungszweckzeilen zugelassen sein).

In Zeile 1 ist die Spenden-/Mitgliedsnummer oder der Name des Spenders einzustellen. Zeile 2 soll Postleitzahl und Straße des Spenders enthalten. In Zeile 3 sind Name und Ort des Kontoinhabers/Einzahlers einzustellen. Die Eingabe der Spenderadresse sollte vom Kundenprodukt wie beschrieben unterstützt werden.

Nr. 10: Ausführungsdatum

Die Belegung ist nicht zugelassen.

Nr. 11: Auftragsidentifikation

Die Belegung ist nicht zugelassen.

◆ Beispiel

```
HKUEB:4:2+1234567:280:10020030+7654321:280:20030
040+AKTION IRGENDWO++100,:DEM+69+000+63519823:12
345 BAHNHOFSTR. 1:FRANZ MEIER, BERLIN'
```

⁵ Vgl. „Richtlinien für einheitliche Zahlungsverkehrsvordrucke und Merkblätter für neutrale Zahlungsverkehrsvordrucke“. Da diese Richtlinien z.Zt. überarbeitet werden, sind eventuelle Änderungen zu berücksichtigen. Es ist zu beachten, daß der Textschlüssel des Vordrucks vom Homebanking-Textschlüssel abweicht.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 11

VII.1.1.2.2 Überweisung mit prüfziffergesicherten Zuordnungsdaten (BZÜ⁶)

◆ Beschreibung

Bei Überweisungen mit prüfziffergesicherten Zuordnungsdaten (z.B. vorausgefüllte Zahlscheine, die den Kunden von Versicherungen zugestellt werden), ist es erforderlich, den Verwendungszweck (exakt 13 Stellen) in der vorgegebenen Form unverändert zu übernehmen (keine Hinzufügungen, Änderungen oder Auslassungen), damit automatisierte Prüfungen beim Kreditinstitut des Auftraggebers durchgeführt werden können und der Zahlungsempfänger die Zahlung zuordnen kann.

Realisierung Bank: verpflichtend, falls auch Einzelüberweisung angeboten wird, sonst optional

Realisierung Kunde: verpflichtend, falls auch Einzelüberweisung angeboten wird, sonst optional



Das korrekte Einreichen einer BZÜ-Überweisung sollte vom Kundenprodukt durch eine gesonderte Eingabemaske unterstützt werden.⁷ Die Auswahl dieser Funktion sollte anhand des Begriffes „BZÜ-Überweisung“ erfolgen. Das Kundenprodukt sollte die Korrektheit des Verwendungszwecks in der oben dargestellten Form prüfen und vor dem Versenden des Auftrags eine einheitliche Prüfziffernkontrolle nach DIN ISO 7064, MOD 11,10 durchzuführen.⁸ Falls diese Prüfung fehlschlägt, sollte das Kundenprodukt den Kunden auffordern, die eingegebenen Zuordnungsdaten zu korrigieren. Bei erneutem Fehlschlagen der Prüfziffernkontrolle kann die Überweisung dennoch (mit Textschlüssel 67) an das Kreditinstitut übermittelt werden. In diesem Fall wird das Kreditinstitut diese Überweisung nicht ablehnen, sondern mit Textschlüssel 68 unter Hinzunahme des Auftraggebernamens zwischenbetrieblich weiterleiten.

◆ Format

Name: BZÜ-Überweisung
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HKUEB
 Bezugssegment: -
 Segmentversion: 2
 Sender: Kunde
 Format: Einzelauftrag Inlandszahlungsverkehr

⁶ Speziell gestaltetes Zahlscheinüberweisungsformular, das der Zahlungsempfänger dem Zahlungspflichtigen maschinell vorausgefüllt zur Verfügung stellt.

⁷ Zur optischen Gestaltung s. Abb. 13 in „Richtlinien für einheitliche Zahlungsverkehrsvordrucke und Merkblätter für neutrale Zahlungsverkehrsvordrucke“. Da diese Richtlinien z.Zt. überarbeitet werden, sind eventuelle Änderungen zu berücksichtigen. Es ist zu beachten, daß der Textschlüssel des Vordrucks vom Homebanking-Textschlüssel abweicht.

⁸ s. Kap VIII.10

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 12	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

♦ Belegungsrichtlinien

Nr. 7: Textschlüssel

Es muß der Wert '67' eingestellt werden.

Nr. 9: Verwendungszweck

In die erste Verwendungszweckzeile sind die 13-stelligen prüfziffergesicherten Zuordnungsdaten einzustellen.

Nr. 10: Ausführungsdatum

Die Belegung ist nicht zugelassen.

Nr. 11: Auftragsidentifikation

Die Belegung ist nicht zugelassen.

♦ Beispiel

```
HKUEB:4:2+1234567:280:10020030+7654321:280:20030
040+MEIER FRANZ++100,:DEM+67+000+1234567890123'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 13

VII.1.1.3 Terminierte Überweisung

Folgende Geschäftsvorfälle sind vorgesehen:

- Einreichung terminierter Überweisungen
- Änderung terminierter Überweisungen
- Bestand terminierter Überweisungen abrufen
- Löschung terminierter Überweisungen

Die Abbildung zeigt die Abfolge der Geschäftsvorfälle:

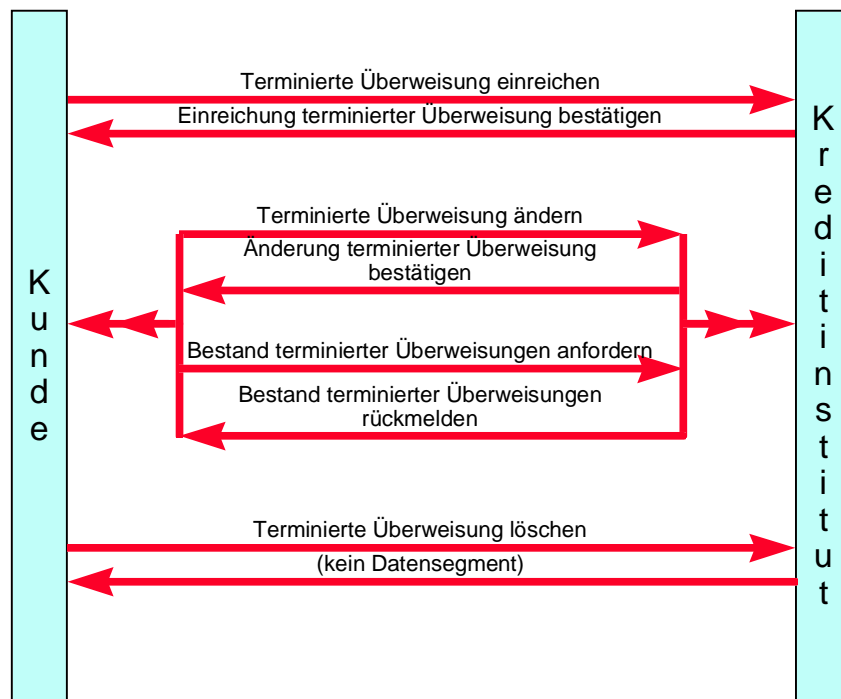


Abb. 19: Lebenszyklus einer terminierten Überweisung

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 14	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

VII.1.1.3.1 Einreichung terminierter Überweisungen

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Terminierte Überweisung einreichen
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKTUE
Bezugssegment: -
Segmentversion: 2
Sender: Kunde
Format: Einzelauftrag Inlandszahlungsverkehr

◆ Belegungsrichtlinien

Nr. 10: Ausführungsdatum

Das DE muß belegt werden. Es ist das Ausführungsdatum einzustellen.

Nr. 11: Auftragsidentifikation

Die Belegung ist nicht zugelassen.

◆ Beispiel

```
HKTUE:3:2+1234567:280:10020030+7654321:280:20030
040+MEIER FRANZ++1000,:DEM+51+000+RE-NR.1234:KD-
NR.9876+19960701'
```

b) Kreditinstitutsrückmeldung

◆ Format

Name: Einreichung terminierter Überweisung bestätigen
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HITUE
Bezugssegment: HKTUE
Segmentversion: 2
Sender: Kreditinstitut

Nr.	Name	Typ	For- mat	Län- ge	Sta- tus	An- zahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Auftragsidentifikation	DE	an	..99	K	1	

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 15

◆ Erläuterungen

Nr. 2: Auftragsidentifikation

Die Auftragsidentifikation wird bspw. als Referenz für die Änderung und Löschung der terminierten Überweisung verwendet.



Falls das Kreditinstitut schon bei der Einreichung eine Auftragsidentifikation zurückmelden kann, sollte diese Möglichkeit genutzt werden. Andernfalls hat das Kundensystem vor einer Änderung oder Löschung den gesamten Bestand abzurufen (s. VII.1.1.3.3 „Bestand terminierter Überweisungen abrufen“), um in den Besitz der Auftragsidentifikation zu gelangen.

◆ Beispiel

HITUE:3:2:3+00001'

◆ Ausgewählte Beispiele für RückmeldungsCodes

Zusätzlich zu den RückmeldungsCodes der Einzelüberweisung gelten:

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
0020	Auftrag zur Ausführung vorgemerkt
3030	Datum ist kein Bankgeschäftstag. Der Auftrag wird ausgeführt am ...
9210	Mindestzeitraum bis zum Ausführungstermin überschritten
9210	Datum liegt nicht in der Zukunft
9210	Datum liegt zu weit in der Zukunft
9210	Datum ist kein Buchungstag

c) Bankparameterdaten

◆ Format

Name: Terminierte Überweisung einreichen Parameter
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HITUES
Bezugssegment: HKVVB
Segmentversion: 2
Sender: Kreditinstitut
Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter terminierte Überweisung einreichen
Typ: Datenelementgruppe

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 16	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Minimale Vorlaufzeit	GD	num	..4	M	1	
2	Maximale Vorlaufzeit	GD	num	..4	M	1	
3	Maximale Anzahl Verwendungszweckzeilen	GD	num	..2	M	1	
4	Textschlüssel	GD	dig	2	M	1..99	

Nr. 1: Minimale Vorlaufzeit

Zeitraum, den ein terminierter Auftrag vor seiner Ausführung eingereicht werden muß. Die Angabe erfolgt in Tagen. Der minimale Wert beträgt 0.

Nr. 2: Maximale Vorlaufzeit

Zeitraum, für den terminierte Aufträge im voraus erteilt werden können. Die Angabe erfolgt in Tagen. Wird hier z.B. "90" eingestellt, kann der Kunde Aufträge für 3 Monate im voraus einreichen. Die maximale Vorlaufzeit muß größer oder gleich der minimalen Vorlaufzeit sein.

Nr. 3: Maximale Anzahl Verwendungszweckzeilen

Es ist die maximale Anzahl der Verwendungszweckzeilen einzustellen, die der Kunde im Rahmen einer terminierten Überweisung belegen darf. Diese Anzahl hat sich an den DTA-Richtlinien zu orientieren (z.Zt. 0-14).

Nr. 4: Textschlüssel

Einzustellen sind die vom Kreditinstitut unterstützten Textschlüssel.¹ Hierzu gehört mindestens der Textschlüssel 51 („Überweisungsgutschrift“). Weiterhin sind gemäß den Vorgaben für die Sonderformen der Überweisung (vgl. Kap. VII.1.1.2) auch die Textschlüssel 67 und 69 Pflicht.

◆ Beispiel

HITUES:8:2:5+1+2+1:45:14:51:53:54:67:69'

¹ Ein Verzeichnis aller grundsätzlich für die Belegung durch den Kunden erlaubten Textschlüssel und Textschlüsselergänzungen befindet sich in der Anlage zum DTAUS-Format (Kap. VIII.9.1).

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 17

VII.1.1.3.2 Änderung terminierter Überweisungen



Dieser Geschäftsvorfall darf vom Kreditinstitut nur angeboten werden, wenn es eine Auftragsidentifikation unterstützt, da ansonsten die Identifikation der zu ändernden Überweisung nicht möglich ist.



Vor der Änderung einer terminierten Überweisung hat eine Abholung des aktuellen Bestandes beim Kreditinstitut (s.u.) zu erfolgen, um sicherzustellen, daß der Kunde auf Basis des korrekten Bestandes operiert. Nur so ist gewährleistet, daß zwischenzeitliche Änderungen auf anderem Wege (z.B. schriftlich oder per Selbstbedienungsterminal) von der Kundensoftware berücksichtigt werden.



Falls dieser Geschäftsvorfall kreditinstitutsseitig oder vom Kundenprodukt nicht angeboten wird, kann durch den Kunden eine Änderung erreicht werden, indem er die terminierte Überweisung löscht und anschließend neu einreicht.

Realisierung Bank: optional
Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Terminierte Überweisung ändern
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKTUA
Bezugssegment: -
Segmentversion: 2
Sender: Kunde
Format: Einzelauftrag Inlandszahlungsverkehr

◆ Belegungsrichtlinien

Die Felder sind so zu belegen, wie die terminierte Überweisung nach der Änderung ausgeführt werden soll, d.h. es sind nicht nur die zu ändernden Felder zu belegen. Die gleichzeitige Änderung mehrerer Felder ist möglich.

Nr. 11: Auftragsidentifikation

Das DE muß belegt werden. Es ist das vom Kreditinstitut mitgeteilte Identifikationsmerkmal des Auftrags einzustellen.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 18	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

◆ Beispiel

```
HKTUA:3:2+1234567:280:10020030+7654321:280:20030
040+MEIER FRANZ++2000,:DEM+51+000+RE-NR.1234:KD-
NR.9876+19960801+00001'
```

b) Kreditinstitutsrückmeldung

◆ Format

Name: Änderung terminierter Überweisung bestätigen
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HITUA
 Bezugssegment: HKTUA
 Segmentversion: 2
 Sender: Kreditinstitut

Nr.	Name	Typ	Form- at	Län- ge	Sta- tus	An- zahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Auftragsidentifikation	DE	an	..99	M	1	
3	Auftragsidentifikation alt	DE	an	..99	K	1	

◆ Erläuterungen

Nr. 2: Auftragsidentifikation

Es ist die für diese terminierte Überweisung aktuell gültige Auftragsidentifikation anzugeben.

Nr. 3: Auftragsidentifikation alt

In der Regel wird die Auftragsidentifikation einer terminierten Überweisung durch einen Änderungsauftrag nicht modifiziert. Dies ist jedoch möglich, wenn z.B. die Änderung bankseitig durch eine Löschung und Neueinreichung realisiert wird. In diesem Fall muß dem Kundensystem im DE „Auftragsidentifikation“ die neu vergebene und im DE „Auftragsidentifikation alt“ aus Zuordnungsgründen die bisherige Auftragsidentifikation mitgeteilt werden. Falls keine Änderung der Auftragsidentifikation stattgefunden hat, ist das DE nicht zu belegen.



Falls eine neue Auftragsidentifikation vergeben wurde, ist der lokale Bestand im Kundenprodukt zu aktualisieren.

◆ Beispiel

```
HITUA:3:2:3+00002+00001'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 19

♦ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
0020	Auftrag ausgeführt
9010	Auftrag zur Zeit nicht änderbar
9010	Auftrag bereits zur Löschung vorgemerkt
9010	Auftrag inkonsistent
9160	Auftragsidentifikation fehlt
9210	Datum liegt zu weit in der Zukunft
9210	Datum liegt nicht in der Zukunft
9210	Auftrag existiert nicht, Auftragsidentifikation unbekannt
9210	Kontonummer des Auftraggebers darf nicht geändert werden
9210	Das angegebene Datum ist kein Ausführungsdatum

c) Bankparameterdaten

♦ Format

Name: Terminierte Überweisung ändern Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HITUAS
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

♦ Erläuterungen

Nr. 4: Parameter

Name: Parameter terminierte Überweisung ändern
 Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Minimale Vorlaufzeit	GD	num	..4	M	1	
2	Maximale Vorlaufzeit	GD	num	..4	M	1	
3	Maximale Anzahl Verwendungszweckzeilen	GD	num	..2	M	1	
4	Textschlüssel	GD	dig	2	M	1..99	

Erläuterungen s. „Einreichung terminierter Überweisungen“. Die Parameter der Änderung müssen nicht mit denen der Einreichung übereinstimmen.

♦ Beispiel

HITUAS:9:2:5+1+2+1:45:14:51:53:54:67:69'

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 20	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

VII.1.1.3.3 Bestand terminierter Überweisungen abrufen

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Beschreibung

Der Kunde ruft die im Kreditinstitut zu einem Konto hinterlegten terminierten Aufträge ab, die noch zur Ausführung anstehen.

◆ Format

Name: Bestand terminierter Überweisungen anfordern
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKTUB
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kontoverbindung Auftraggeber	DEG	kto	#	M	1	
3	Von Datum	DE	dat	#	K	1	
4	Bis Datum	DE	dat	#	K	1	
5	Maximale Anzahl Einträge	DE	num	..4	K	1	>0
6	Aufsetzpunkt	DE	an	..35	K	1	

◆ Erläuterungen

Nr. 2: Kontoverbindung Auftraggeber

Es ist die Kontoverbindung anzugeben, für die die noch zur Ausführung anstehenden terminierten Aufträge angefordert werden.

Nr. 3,4: Von Datum, Bis Datum

Es werden alle terminierten Aufträge zurückgemeldet, deren Ausführung im angegebenen Zeitraum ansteht. Sollten Kreditinstitute keine Auswahlmöglichkeit haben und alle noch nicht ausgeführten Aufträge übermitteln, so ist dies in den BPD hinterlegt. In diesem Fall darf kein Zeitraum angegeben werden. Andernfalls können die DE belegt werden, wie in Kap. II.7.3 („Von Datum, Bis Datum“) beschrieben.

Nr. 5: Maximale Anzahl Einträge

Es kann die Anzahl der rückzumeldenden terminierten Überweisungen begrenzt werden (s. Kap. II.7.3).

Nr. 6: Aufsetzpunkt

Belegung nur zulässig, wenn vom Kreditinstitut ein Aufsetzpunkt rückgemeldet wurde (s. Kap. II.7.3).

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 21

♦ Beispiel

```
HKTUB:3:1+1234567:280:10020030+19960701+19960731
'
```

b) Kreditinstitutsrückmeldung

♦ Beschreibung

Für jeden terminierten Überweisungsauftrag wird ein entsprechendes Datensegment in die Rückmeldungsnachricht eingestellt.

♦ Format

Name: Bestand terminierter Überweisungen rückmelden
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HITUB
 Bezugssegment: HKTUB
 Segmentversion: 1
 Sender: Kreditinstitut
 Format: Einzelauftrag Inlandszahlungsverkehr

♦ Belegungsrichtlinien

Nr. 10: Ausführungsdatum

Das DE muß belegt werden. Es ist das Ausführungsdatum einzustellen.

Nr. 11: Auftragsidentifikation

Falls das Kreditinstitut eine Auftragsidentifikation vergeben hat, ist diese hier einzustellen.

♦ Beispiel

```
HITUB:3:1:5+1234567:280:10020030+7654321:280:200
30040+MEIER FRANZ++1000,:DEM+51+000+RE-NR.12345+
19960701+00001 '

HITUB:4:1:5+1234567:280:10020030+54321:280:30040
050+SPORTVEREIN E.V.+MUSTERSTADT+100,:DEM+51+000
+JAHRESBEITRAG+19960705+00002 '
```

♦ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
3010	Es liegen keine Einträge vor
9210	Bereichende darf nicht vor Bereichanfang liegen
9210	Datum liegt nicht in der Zukunft
9210	Keine gültige Kontonummer des Kunden

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 22	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

c) Bankparameterdaten

◆ Format

Name: Bestand terminierter Überweisungen Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HITUBS
 Bezugssegment: HKVVB
 Segmentversion: 1
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Bestand terminierter Überweisungen
 Type: Datenelementgruppe

Nr.	Name	Typ	For- mat	Län- ge	Sta- tus	An- zahl	Restriktionen
1	Zeitraum möglich	GD	jn	#	M	1	

Nr. 1: Zeitraum möglich

Falls der Kunde im Auftrag einen Zeitraum angeben kann, ist hier 'J' einzustellen. Können Kreditinstitute jedoch nur alle noch nicht ausgeführten Aufträge übermitteln, so ist 'N' einzustellen.

◆ Beispiel

HITUBS:10:1:5+1+2+J '

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 23

VII.1.1.3.4 Löschung terminierter Überweisungen

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Beschreibung

Die zu löschende Überweisung wird über eine Auftragsidentifikation, die beim Abruf des Bestandes mitübertragen wird, bestimmt. Neben der Auftragsidentifikation müssen auch die restlichen Auftragsdaten eingestellt werden, um kreditinstitutsseitig Plausibilitätsprüfungen zu ermöglichen.



Dieser Geschäftsvorfall darf vom Kreditinstitut nur angeboten werden, wenn es eine Auftragsidentifikation unterstützt, da ansonsten die Identifikation der zu löschenden Überweisung nicht möglich ist.

Zu löschende terminierte Aufträge liegen immer in der Zukunft. Eine minimale Vorlaufzeit für die Einreichung des Löschauftrags ist nicht vorgesehen. Es können jedoch nur Aufträge gelöscht werden, die auch im Bestand aufgeführt werden.

◆ Format

Name: Terminierte Überweisung löschen
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HKTUL
 Bezugssegment: -
 Segmentversion: 1
 Sender: Kunde
 Format: Einzelauftrag Inlandszahlungsverkehr

◆ Belegungsrichtlinien

Nr. 10: Ausführungsdatum

Das DE muß belegt werden. Es ist das **aktuell gültige** Ausführungsdatum **der terminierten Überweisung** einzustellen.

Nr. 11: Auftragsidentifikation

Das DE muß belegt werden. Es ist das vom Kreditinstitut mitgeteilte Identifikationsmerkmal des Auftrags einzustellen.

◆ Beispiel

```
HKTUL:3:1+1234567:280:10020030+7654321:280:20030
040+MEIER FRANZ++1000,:DEM+51+000+RE-NR.1234:KD-
NR. 9876+19960701+00001'
```

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 24	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

b) Kreditinstitutsrückmeldung

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

◆ Ausgewählte Beispiele für Rückmeldungscodes

Code	Beispiel für Rückmeldungstext
0010	Auftrag zur Löschung vorgemerkt
0020	Auftrag gelöscht
9010	Löschung nicht mehr möglich, da Auftrag bereits zur Löschung vorgemerkt
9010	Auftragsidentifikation stimmt nicht mit Auftragsdaten überein
9210	Auftrag existiert nicht bzw. wurde bereits ausgeführt

c) Bankparameterdaten

◆ Format

Name: Terminierte Überweisung löschen Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HITULS
 Bezugssegment: HKVVB
 Segmentversion: 1
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Die DEG wird nicht belegt.

◆ Beispiel

HITULS:11:1:5+1+2 '

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 25

VII.1.1.4 Dauerauftrag

Folgende Geschäftsvorfälle sind vorgesehen:

- Einrichtung eines Dauerauftrags
- Ändern eines Dauerauftrags
- Dauerauftragsaussetzung
- Bestandsabfrage
- Abruf von Dauerauftragsänderungsvormerkungen
- Dauerauftragslöschung

Die Abbildung zeigt die Abfolge der Geschäftsvorfälle im Dauerauftragsbereich:

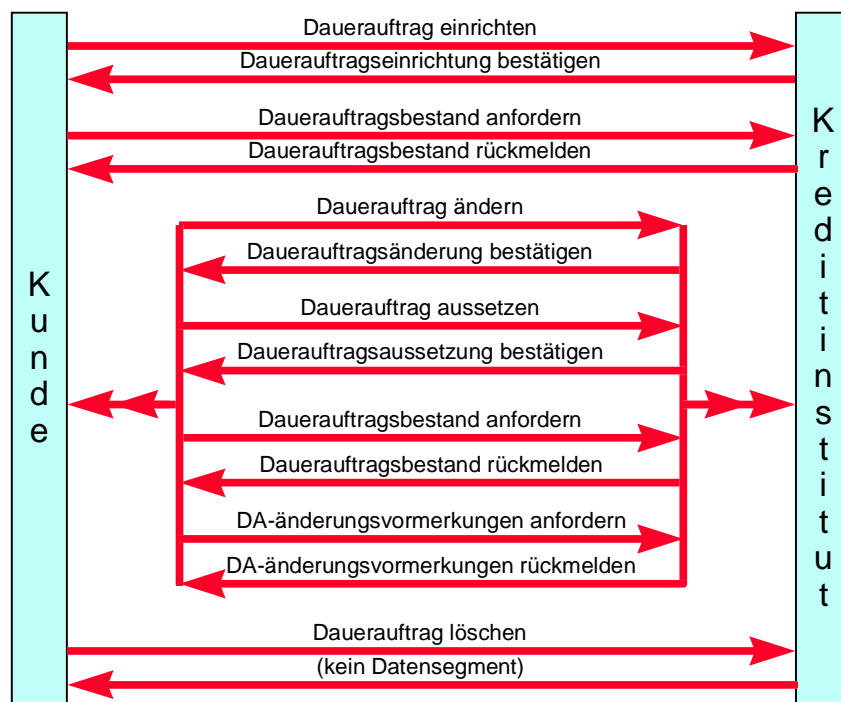


Abb. 20: Lebenszyklus Dauerauftrag

Daueraufträge sind z.Zt. nur für den Inlandszahlungsverkehr vorgesehen. Die umfangreiche Komplexität sämtlicher Dauerauftragsmodalitäten kann im Rahmen dieser Schnittstelle nicht abgebildet werden. Derartige Verarbeitungsvorgänge können statt dessen evtl. durch die Steuerung des Kundenprodukts abgewickelt werden.



Von den hier dargestellten Aufträgen zu unterscheiden sind vom Kundenprodukt verwaltete Daueraufträge, d.h. Einzelaufträge, bei denen das Kundensystem die Terminverwaltung und regelmäßige Versendung übernimmt. Diese können für den Kunden insbesondere dann eine Alternative darstellen, falls entweder das Kundenprodukt oder das Kreditinstitut keine Dauerauftragsverwaltung anbietet.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 26	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland



Die Geschäftsvorfälle „Dauerauftragsänderung“, „Dauerauftragsaussetzung“ und „Dauerauftragsänderungsvormerkungen abrufen“ dürfen vom Kreditinstitut nur angeboten werden, wenn es eine Auftragsidentifikation unterstützt, da ansonsten die Identifikation des zu ändernden Dauerauftrags nicht möglich ist.



Vor der Modifikation eines Dauerauftrages (Änderung, Aussetzung) hat eine Abholung des aktuellen Bestandes bzw. der Änderungsvormerkungen beim Kreditinstitut (s.u.) zu erfolgen, um sicherzustellen, daß der Kunde auf Basis des korrekten Bestandes operiert. Nur so ist gewährleistet, daß zwischenzeitliche Änderungen auf anderem Wege (z.B. schriftlich oder per Selbstbedienungsterminal) von der Kundensoftware berücksichtigt werden.

Das Datenformat für Daueraufträge entspricht dem Format für Einzelaufträge im Inlandszahlungsverkehr. Es wird ergänzt um dauerauftragspezifische Informationen.

◆ Format

Name: Dauerauftrag
Typ: Format

Zur Erläuterung s. Format „Einzelauftrag Inlandszahlungsverkehr“.

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kontoverbindung Auftraggeber	DEG	kto	#	M	1	
3	Kontoverbindung Empfänger/Zahlungspflichtiger	DEG	kto	#	M	1	
4	Name Empfänger/Zahlungspflichtiger 1	DE	an	..27	M	1	
5	Name Empfänger/Zahlungspflichtiger 2	DE	an	..27	K	1	
6	Betrag	DEG	btg	#	M	1	
7	Textschlüssel	DE	dig	2	M	1	
8	Textschlüsselergänzung	DE	dig	3	K	1	
9	Verwendungszweck	DEG			K	1	
10	Ausführungsdatum	DE	dat	#	K	1	
11	Auftragsidentifikation	DE	an	..99	K	1	
12	Dauerauftragdetails	DEG			M	1	
13	Aussetzung	DEG			K	1	

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 27

◆ Format

Name: Dauerauftragdetails
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Erstmals ausführen am	GD	dat	#	M	1	
2	Zeiteinheit	GD	an	1	M	1	W, M
3	Turnus	GD	num	..2	M	1	>0
4	Ausführungstag	GD	num	..2	M	1	>0
5	Letztmals ausführen am	GD	dat	#	K	1	

Nr. 1: Erstmals ausführen am

Legt das Datum der erstmaligen Ausführung des Dauerauftrags fest. Es muß sich um ein erlaubtes Ausführungsdatum im Sinne des angegebenen Turnus handeln.

Der mögliche Wertebereich wird durch die DE „Minimale Vorlaufzeit“ und „Maximale Vorlaufzeit“ aus der BPD vorgegeben.



Die Errechnung möglicher Ausführungsdaten bzw. die Prüfung auf Gültigkeit des vom Kunden eingegebenen Datums kann vom Kundenprodukt übernommen werden.

Nr. 2: Zeiteinheit

Gibt die Zeiteinheit an, auf das sich die Angabe im DE "Turnus" bezieht:

Zeiteinheit	Bedeutung
M	Monat
W	Woche

Es darf nur ein gemäß BPD zugelassener Wert eingestellt werden.

Nr. 3: Turnus

Gibt die Anzahl der Zeiteinheiten an, die zwischen 2 Ausführungen eines Dauerauftrages liegen sollen.

Wertebereich:

Zeiteinheit	Turnus
M	1 bis 12
W	1 bis 52

Ein Turnus von mehr als einem Jahr ist nicht zulässig.

Es darf nur ein gemäß BPD zugelassener Wert eingestellt werden.

Die Gültigkeit der Kombination aus Zeiteinheit und Turnus ergibt sich aus den Vorgaben in der BPD:

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 28	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

Beispiele:

Zeit- einheit	Tur- nus	Bedeutung
M	1	Monatliche Ausführung
M	3	Vierteljährliche Ausführung
M	12	Jährliche Ausführung
W	1	Wöchentliche Ausführung
W	2	Ausführung alle 2 Wochen

Nr. 4: Ausführungstag

Durch dieses Feld wird bei monatlichem Turnus der regelmäßige Kalendertag der Ausführung und bei wöchentlichem Turnus der regelmäßige Wochentag der Ausführung festgelegt.

Es dürfen nur erlaubte Ausführungstage eingestellt werden. Die je Kreditinstitut zugelassenen Ausführungstage pro Monat bzw. pro Woche sind in der BPD eingestellt.

Nr. 5: Letztmals ausführen am

Dieses DE legt den letzten Ausführungstermin fest. Die Belegung ist optional. Es muß sich um ein erlaubtes Ausführungsdatum im Sinne des angegebenen Turnus handeln. Die je Kreditinstitut erlaubten Ausführungsdaten sind in der BPD eingestellt.

Beispiele:

Erstmals aus- führen am	Zeit- einheit	Tur- nus	Ausfüh- rungstag	Bedeutung
19970215	M	1	15	erstmalig am 15.2.1997, danach jeweils zum 15. eines Monats
19970215	M	2	15	erstmalig am 15.2.1997, danach alle 2 Monate jeweils zum 15. eines Monats
19970210	W	1	1	erstmalig am Montag, den 10.2.1997, danach jeweils montags
19970210	W	4	1	erstmalig am Montag, den 10.2.1997, danach alle 4 Wochen jeweils montags
19970228	M	1	30	erstmalig am 28.2.1997, danach jeweils zum 30. eines Monats (die Ausführung in Monaten mit weniger als 30 Tagen ist kreditinstitutsindividuell zu behandeln)
19970228	M	1	99	erstmalig am 28.2.1997, danach jeweils zum Ultimo eines Monats (31.03., 30.04. etc.)

◆ Format

Name: Aussetzung
Typ: Datenelementgruppe

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 29

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Aussetzung jährlich wiederkehrend	GD	jn	#	M	1	
2	Aussetzen von	GD	dat	#	K	1	
3	Aussetzen bis	GD	dat	#	K	1	
4	Anzahl Aussetzungen	GD	num	..2	K	1	

Nr. 1: Aussetzung jährlich wiederkehrend

Ob jährlich wiederkehrende Aussetzungen zulässig sind, teilt das Kreditinstitut in den BPD mit. Falls ja, kann der Kunde hier wählen, ob die Aussetzung nur einmalig oder jährlich wiederkehrend (z.B. jedes Jahr von Februar bis August) ausgeführt werden soll. Falls nein, ist das DE mit 'N' zu belegen.

Nr. 2: Aussetzen von

Falls terminierte Aussetzungen erlaubt sind (s. BPD), ist hier ist das Datum der erstmaligen Aussetzung des Dauerauftrages einzustellen. Es muß sich dabei um ein gültiges Datum handeln, zu dem eine Ausführung stattfinden würde. Ist das DE nicht eingestellt, so wird der Dauerauftrag erstmalig zum nächsten Ausführungstermin ausgesetzt. Falls die Terminierung von Aussetzungen nicht erlaubt ist, darf das DE nicht belegt werden.

Nr. 3: Aussetzen bis

Es gibt zwei Möglichkeiten, die Ausführung des Dauerauftrages für einen bestimmten Zeitraum zu unterbrechen. Welche Varianten vom Kreditinstitut unterstützt werden, erfährt der Kunde in der BPD.

Bei der ersten Variante ist hier das Datum einzustellen, zu dem der Dauerauftrag das letzte Mal nicht ausgeführt werden soll. Es muß sich um ein gültiges Ausführungsdatum im Sinne des angegebenen Turnus handeln.

Ist dieses DE belegt, so ist die Belegung des DE „Anzahl Aussetzungen“ nicht zulässig.

Beispiel:

Der Dauerauftrag soll letztmalig am 1.6. ausgeführt werden. Die Ausführung soll zum 1.10. wiederaufgenommen werden.

Datenelement	Wert
Aussetzen von	19960701
Aussetzen bis	19960901

Nr. 4: Anzahl Aussetzungen

Bei der zweiten Variante kann der Kunde hier die Anzahl der gewünschten Aussetzungen seines Dauerauftrags angeben. Ist dieses DE belegt, so ist die Belegung des DE „Aussetzen bis“ nicht zulässig.

Beispiel:

Der Dauerauftrag soll letztmalig am 1.6. ausgeführt werden. Die Ausführung soll zum 1.10. wiederaufgenommen werden.

Datenelement	Wert
Aussetzen von	19960701
Anzahl Aussetzungen	3

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 30	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

VII.1.1.4.1 Dauerauftragseinrichtung

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Dauerauftrag einrichten
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKDAE
Bezugssegment: -
Segmentversion: 2
Sender: Kunde
Format: Dauerauftrag

◆ Belegungsrichtlinien

Nr. 10: Ausführungsdatum

Dieses DE darf bei der Dauerauftragseinreichung nicht belegt werden. Das Datum der ersten Ausführung wird statt dessen durch das DE „Erstmals ausführen am“ angegeben. Dieses DE wird nur für nachträgliche Dauerauftragsänderungen genutzt.

Nr. 11: Auftragsidentifikation

DE darf bei der Dauerauftragseinreichung nicht belegt werden.

Nr. 13: Aussetzung

Bei der Einreichung eines Dauerauftrags darf keine Aussetzung angegeben werden.

◆ Beispiel

```
HKDAE:3:2+1234567:280:10020030+7654321:280:20030
040+MEIER FRANZ++1000,:DEM+52+000+MIETE:UND NEBE
NKOSTEN+++19960701:M:1:1:19970601'
```

b) Kreditinstitutsrückmeldung

◆ Format

Name: Dauerauftragseinrichtung bestätigen
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HIDAE
Bezugssegment: HKDAE
Segmentversion: 2
Sender: Kreditinstitut

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 31

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Auftragsidentifikation	DE	an	..99	K	1	

◆ Erläuterungen

Nr. 2: Auftragsidentifikation

Die Auftragsidentifikation (Dauerauftragsnummer) wird bspw. als Referenz für die Änderung und Löschung des Dauerauftrags verwendet.



Falls das Kreditinstitut schon bei der Einreichung eine Auftragsidentifikation zurückmelden kann, sollte diese Möglichkeit genutzt werden. Andernfalls hat das Kundensystem vor einer Änderung oder Löschung den gesamten Bestand abzurufen (s. VII.1.1.4.4 „Dauerauftragsbestand abrufen“), um in den Besitz der Auftragsidentifikation zu gelangen.

◆ Beispiel

HIDAE:3:2:3+00001'

◆ Ausgewählte Beispiele für RückmeldungsCodes

Es sind sämtliche RückmeldungsCodes des Geschäftsvorfalles „Einzelüberweisung“ und „Einreichung terminierter Überweisung“ möglich: Zusätzlich gelten:

Code	Beispiel für Rückmeldungstext
9210	Der angegebene Turnus ist kein Ausführungsturnus

c) Bankparameterdaten

◆ Beschreibung

Das Kreditinstitut gibt die monatlich bzw. wöchentlich erlaubten Ausführungsrythmen an. In den Datenelementen 4 bis 6 sind die unterstützten Werte in aufsteigender Reihenfolge als Kette 2-stelliger Zahlen einzustellen. Die DE-Länge von 62 würde somit die Eingabe aller Tage eines Monats erlauben.

◆ Format

Name: Dauerauftrag einrichten Parameter
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HIDAES
Bezugssegment: HKVVB
Segmentversion: 2
Sender: Kreditinstitut
Format: Geschäftsvorfallparameter

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 32	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Dauerauftrag einrichten

Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Maximale Anzahl Verwendungszweckzeilen	GD	num	..2	M	1	
2	Minimale Vorlaufzeit	GD	num	..4	M	1	
3	Maximale Vorlaufzeit	GD	num	..4	M	1	
4	Turnus in Monaten	GD	dig	..24	M	1	
5	Ausführungstage pro Monat	GD	dig	..64	M	1	
6	Turnus in Wochen	GD	dig	..104	K	1	
7	Ausführungstage pro Woche	GD	dig	..7	K	1	
8	Textschlüssel	GD	dig	2	M	1..99	

Nr. 1: Maximale Anzahl Verwendungszweckzeilen

Es ist die maximale Anzahl der Verwendungszweckzeilen einzustellen, die der Kunde im Rahmen eines Dauerauftrags belegen darf. Diese Anzahl hat sich an den DTA-Richtlinien zu orientieren (z.Zt. 0-14).

Nr. 2: Minimale Vorlaufzeit

Zeitraum, den ein Dauerauftrag vor seiner erstmaligen Ausführung mindestens eingereicht werden muß. Die Angabe erfolgt in Tagen. Der minimale Wert beträgt 0.

Nr. 3: Maximale Vorlaufzeit

Zeitraum, für den ein Dauerauftrag vor seiner ersten Ausführung maximal im voraus eingereicht werden kann. Die Angabe erfolgt in Tagen. Wird hier z.B. 60 eingestellt, kann der Kunde Aufträge für 2 Monate im voraus einreichen. Die maximale Vorlaufzeit muß größer oder gleich der minimalen Vorlaufzeit sein.

Nr. 4: Turnus in Monaten

Erlaubt sind 00 (alle Möglichkeiten) oder 01 (monatlich) bis 12 (jährlich).

Bsp.: 0102030612 (Ausführung monatlich, 2-monatlich, vierteljährlich, halbjährlich und jährlich möglich)

Nr. 5: Ausführungstage pro Monat

Erlaubt sind 00 (alle) oder 01 bis 30 oder 97 (Ultimo-2), 98 (Ultimo-1) und 99 (Ultimo).¹

Bsp.: 01101520259899 (Ausführung am 1., 10., 15., 20. und 25. jeden Monats, sowie zum Ultimo und Ultimo-1 möglich)

Nr. 6: Turnus in Wochen

Erlaubt sind 00 (alle Möglichkeiten) oder 01 bis 52.

¹ Der 31. eines Monats ist als Ultimo (99) zu kodieren.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 33

Bsp.: 01020408 (Ausführung wöchentlich, 2-wöchentlich, alle 4 Wochen und alle 8 Wochen möglich)

Wenn das DE nicht belegt ist, ist keine wöchentliche Ausführung möglich.

Nr. 7: Ausführungstage pro Woche

Erlaubt sind 0 (täglich) oder 1 (montags) bis 7 (sonntags).

Bsp.: 12345 (Ausführung an allen Werktagen möglich)

Das Feld muß eingestellt werden, wenn auch das Feld 'Turnus in Wochen' belegt ist. Es darf nicht eingestellt werden, wenn das Feld 'Turnus in Wochen' nicht belegt ist.

Nr. 8: Textschlüssel

Einzustellen sind die vom Kreditinstitut für Daueraufträge unterstützten Textschlüssel (s. auch VII.1.1).² Verpflichtend ist der Textschlüssel 52 (Dauerauftrags-Gutschrift).

◆ Beispiel

```
HIDAES:12:2:5+1+2+14:1:60:00:01101520259899:0102
0304:12:52:54'
```

² Ein Verzeichnis aller grundsätzlich für die Belegung durch den Kunden erlaubten Textschlüssel und Textschlüsselergänzungen befindet sich in der Anlage zum DTAUS-Format (Kap. VIII.9.1).

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 34	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

VII.1.1.4.2 Dauerauftragsänderung

Das Kreditinstitut teilt in den BPD mit, welche Felder durch den Kunden änderbar sind. Die Auftragsidentifikation und die Auftraggeberkontoverbindung sind grundsätzlich nicht änderbar.

Änderungen gelten, sofern nichts anderes bestimmt ist, zum nächsten Ausführungstermin. Darüber hinaus kann das Kreditinstitut in den BPD festsetzen, ob es zusätzlich terminierte Änderungen erlaubt. In diesem Fall ist weiterhin möglich, daß das Kreditinstitut nur eine oder mehrere terminierte Änderungen gleichzeitig zuläßt.



Falls dieser Geschäftsvorfall kreditinstitutsseitig oder vom Kundenprodukt nicht angeboten wird, kann durch den Kunden eine Änderung erreicht werden, indem er den Dauerauftrag löscht und anschließend neu einreicht. Dasselbe gilt für den Fall, daß die Änderung eines nicht änderbaren Feldes erforderlich ist.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Beschreibung

Falls das Kreditinstitut keine oder nur jeweils eine terminierte Änderung pro Dauerauftrag zuläßt, sind im Änderungsauftrag vom Kunden stets alle Felder mit den Dauerauftragsdaten zu belegen.

Falls jedoch mehr als eine Änderung zulässig ist, so dürfen von den (gemäß den Angaben in den Bankparameterdaten) änderbaren Feldern nur diejenigen belegt werden, die tatsächlich geändert werden sollen. Die gemäß Bankparameterdaten nicht änderbaren Felder sind in diesem Fall zu belegen, da sie zu Plausibilitätsprüfungen dienen können. Dies ist erforderlich, um Fehldeutungen des Kundenwunsches zu vermeiden.

Beispiel:

Der Kunde richtet am 1.1. einen Dauerauftrag über 1.000 DM zugunsten des Kontos 12345 ein. Am 1.2. sendet er einen terminierten Änderungsauftrag, da er weiß, daß sich der Überweisungsbetrag am 1.7. auf 1.100 DM ändern wird. Am 1.3. erhält er die Information, daß sich die Empfänger-Kontonummer auf 12346 geändert hat und ändert dementsprechend den Dauerauftrag sofort. Sofern der Kunde in seinem ersten Änderungsauftrag sämtliche Auftragsdaten sendet, wird am 1.7. die Kontonummer wieder auf die alte Nummer 12345 zurückgesetzt, d.h. der Kundenwunsch wird falsch interpretiert.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 35

◆ Format

Name: Dauerauftrag ändern
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HKDAN
 Bezugssegment: -
 Segmentversion: 2
 Sender: Kunde
 Format: Dauerauftrag

◆ Belegungsrichtlinien

Nr. 10: Ausführungsdatum

Falls terminierte Änderungen zulässig sind (s. DE „Anzahl terminierter Änderungen“ in den Bankparameterdaten), ist hier ist das Datum der erstmaligen Ausführung des geänderten Dauerauftrages einzustellen. Es muß sich dabei um ein gültiges Ausführungsdatum handeln. Ist das DE nicht eingestellt, so wird die Änderung zum nächstmöglichen Ausführungstermin wirksam. Ist eine terminierte Änderung unzulässig, darf das DE nicht belegt werden. In diesem Fall gilt automatisch der nächstmögliche Ausführungstermin.

Nr. 11: Auftragsidentifikation

Das DE ist mit dem Identifikationsmerkmal zu belegen (Muß-Feld), das vom Kreditinstitut in der Antwortnachricht auf die Dauerauftragseinrichtung oder beim Abholen des Dauerauftragsbestands zurückgemeldet wurde.

Nr. 13: Aussetzung

Darf nicht belegt werden.

◆ Beispiel

```
HKDAN:3:2+1234567:280:10020030++++1100,:DEM++++1
9960901+00001+19960701:::19970601'
```

b) Kreditinstitutsrückmeldung

◆ Format

Name: Dauerauftragsänderung bestätigen
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIDAN
 Bezugssegment: HKDAN
 Segmentversion: 2
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Auftragsidentifikation	DE	an	..99	M	1	
3	Auftragsidentifikation alt	DE	an	..99	K	1	

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 36	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

◆ Erläuterungen

Nr. 2: Auftragsidentifikation

Es ist die für diesen Dauerauftrag aktuell gültige Auftragsidentifikation (Dauerauftragsnummer) anzugeben.

Nr. 3: Auftragsidentifikation alt

In der Regel wird die Auftragsidentifikation eines Dauerauftrags durch einen Änderungsauftrag nicht modifiziert. Dies ist jedoch möglich, wenn z.B. die Änderung bankseitig durch eine Löschung und Neueinreichung realisiert wird. In diesem Fall muß dem Kundensystem im DE „Auftragsidentifikation“ die neu vergebene und im DE „Auftragsidentifikation alt“ aus Zuordnungsgründen die bisherige Auftragsidentifikation mitgeteilt werden. Falls keine Änderung der Auftragsidentifikation stattgefunden hat, ist das DE nicht zu belegen.



Falls eine neue Auftragsidentifikation vergeben wurde, ist der lokale Bestand im Kundenprodukt zu aktualisieren.

◆ Beispiel

HIDAN: 3: 2: 3+00002+00001 '

◆ Ausgewählte Beispiele für Rückmeldungscodes

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
0020	Dauerauftrag geändert
9010	Dauerauftrag zur Zeit nicht änderbar
9010	Änderung bei diesem Dauerauftragstyp nicht möglich
9010	Dauerauftrag bereits zur Löschung vorgemerkt
9010	Auftrag inkonsistent
9160	Auftragsidentifikation fehlt
9210	Aussetzungszeitraum zu groß
9210	Datum liegt zu weit in der Zukunft
9210	Datum liegt nicht in der Zukunft
9210	Dauerauftrag existiert nicht, Auftragsidentifikation unbekannt
9210	Kontonummer des Auftraggebers darf nicht geändert werden

c) Bankparameterdaten

◆ Format

Name: Dauerauftrag ändern Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIDANS
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 37

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Dauerauftrag ändern

Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Anzahl terminierter Änderungen	GD	num	1	M	1	
2	Minimale Vorlaufzeit	GD	num	..4	M	1	
3	Maximale Vorlaufzeit	GD	num	..4	M	1	
4	Kontoverbindung Empfänger änderbar	GD	jn	#	M	1	
5	Empfängername änderbar	GD	jn	#	M	1	
6	Betrag änderbar	GD	jn	#	M	1	
7	Textschlüssel und -ergänzung änderbar	GD	jn	#	M	1	
8	Verwendungszweck änderbar	GD	jn	#	M	1	
9	Erstes Ausführungsdatum änderbar	GD	jn	#	M	1	
10	Zeiteinheit änderbar	GD	jn	#	M	1	
11	Turnus änderbar	GD	jn	#	M	1	
12	Ausführungstag änderbar	GD	jn	#	M	1	
13	Letztes Ausführungsdatum änderbar	GD	jn	#	M	1	
14	Maximale Anzahl Verwendungszweckzeilen	GD	num	..2	M	1	
15	Turnus in Monaten	GD	dig	..24	M	1	
16	Ausführungstage pro Monat	GD	dig	..64	M	1	
17	Turnus in Wochen	GD	dig	..104	K	1	
18	Ausführungstage pro Woche	GD	dig	..7	K	1	
19	Textschlüssel	GD	dig	2	M	1..99	

Nr. 1: Anzahl terminierter Änderungen

Hier ist die maximale Anzahl terminierter Änderungen pro Dauerauftrag einzustellen.

Beispiele:

- 0: Terminierte Änderungen sind nicht erlaubt
- 1: Pro Dauerauftrag ist eine terminierte Änderung erlaubt
- 5: Pro Dauerauftrag sind 5 terminierte Änderungen erlaubt
- 9: keine Beschränkung

Falls mehr als eine terminierte Änderungen erlaubt sind, werden sämtliche Änderungen jeweils zum Ausführungstermin wirksam. Andernfalls führt die Eingabe einer Änderung evtl. zur Überschreibung einer bereits vorher eingegebenen Änderung.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 38	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland



Bei komplexen terminierten Änderungsaufträgen ist es sinnvoll, daß der Kunde mit Hilfe des Geschäftsvorfalles „Dauerauftragsänderungsvormerkungen abrufen“ prüft, ob das Kreditinstitut seinen Änderungswunsch korrekt umgesetzt hat.



Falls der Kundenwunsch nicht eindeutig aus dem Auftrag hervorgeht bzw. zu Inkonsistenzen in der Dauerauftragsverwaltung führt, kann das Kreditinstitut den Auftrag im Zweifel ablehnen. Wenn das Kreditinstitut inkonsistente Aufträge dennoch annehmen möchte, dann darf stets nur der aktuellste Auftrag angenommen werden. Die vorherigen müssen in diesem Fall verworfen werden.

Nr. 2: Minimale Vorlaufzeit

s. Kap. „Dauerauftragseinrichtung“

Nr. 3: Maximale Vorlaufzeit

s. Kap. „Dauerauftragseinrichtung“

Nr. 4-13:

Es ist jeweils einzustellen, ob das betreffende Feld durch den Kunden änderbar ist.

Nr. 9: Erstes Ausführungsdatum änderbar

Sollte das Kreditinstitut die Änderung dieses Feldes zulassen, so ist zu unterscheiden, ob der Änderungsauftrag vor oder nach der ersten Ausführung eingeht:

- In Falle, daß der Dauerauftrag noch nie ausgeführt wurde, wird sofern dieses Feld geändert wird, der erste Ausführungstermin auf den neuen Termin verschoben.
- Falls der Dauerauftrag schon mindestens einmal ausgeführt wurde, wird durch Änderung dieses Feldes der Ausführungstag bzw. -wochentag geändert (s. DE „Erstmals ausführen am“). Es ist zu beachten, daß sich dadurch auch der Ausführungsrhythmus ändern kann.

Nr. 14-19:

s. Kap. „Dauerauftragseinrichtung“. Die Parameter können sich von denen der Dauerauftragseinrichtung unterscheiden.

◆ Beispiel

```
HIDANS:13:2:5+1+2+1:1:60:J:J:J:J:N:N:N:N:N:J:14:
00:01101520259899:01020304:12345:52:54'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 39

VII.1.1.4.3 Dauerauftragsaussetzung

Aussetzungen gelten, sofern nichts anderes bestimmt ist, zum nächsten Ausführungstermin. Darüber hinaus kann das Kreditinstitut in der BPD festsetzen, ob es zusätzlich terminierte Aussetzungen erlaubt.



Falls dieser Geschäftsvorfall vom Kreditinstitut oder vom Kundenprodukt nicht angeboten wird, kann eine Aussetzung auch durch Löschung und terminierte Neueinreichung erreicht werden.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Dauerauftrag aussetzen
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKDAS
Bezugssegment: -
Segmentversion: 1
Sender: Kunde
Format: Dauerauftrag

◆ Belegungsrichtlinien

Es sind die gültigen Daten des Dauerauftrags einzustellen. Diese dienen zu Plausibilitätsprüfungen. Zusätzlich sind folgende Felder wie folgt zu belegen:

Nr. 10: Ausführungsdatum

Falls terminierte Aussetzungen zulässig sind (s. DE „Anzahl terminierter Aussetzungen“ in den Bankparameterdaten), ist hier ist das Datum der erstmaligen Aussetzung des Dauerauftrages einzustellen. Es muß sich dabei um ein gültiges Ausführungsdatum handeln. Ist das DE nicht eingestellt, so wird die Aussetzung zum nächstmöglichen Ausführungstermin wirksam. Ist eine terminierte Aussetzung unzulässig, darf das DE nicht belegt werden. In diesem Fall gilt automatisch der nächstmögliche Ausführungstermin.

Nr. 11: Auftragsidentifikation

Das DE ist mit dem Identifikationsmerkmal zu belegen, das vom Kreditinstitut in der Antwortnachricht auf die Dauerauftragseinrichtung oder beim Abholen des Dauerauftragbestandes zurückgemeldet wurde.

Nr. 13: Aussetzung

Es sind die Aussetzungsdaten einzustellen.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 40	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

◆ Beispiel

```
HKDAS:3:1+1234567:280:10020030+7654321:280:20030
040+MEIER FRANZ++1000,:DEM+52+000+MIETE:UND NEBE
NKOSTEN++00001+19960701:M:1:1:19970601+N:1996090
1:19970101'
```

```
HKDAS:4:1+1234567:280:10020030+7654321:280:20030
040+MEIER FRANZ++1000,:DEM+52+000+MIETE:UND NEBE
NKOSTEN++00002+19960701:M:1:1:19970601+J:1996090
1::4'
```

b) Kreditinstitutsrückmeldung

◆ Format

Name: Dauerauftragsaussetzung bestätigen
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HIDAS
Bezugssegment: HKDAS
Segmentversion: 1
Sender: Kreditinstitut

Nr.	Name	Typ	For- mat	Län- ge	Sta- tus	An- zahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Auftragsidentifikation	DE	an	..99	M	1	
3	Auftragsidentifikation alt	DE	an	..99	K	1	

◆ Erläuterungen

s. „Dauerauftragsänderung bestätigen“

◆ Beispiel

```
HIDAS:3:1:3+00002+00001'
```

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
0020	Dauerauftrag ausgesetzt
9010	Dauerauftrag zur Zeit nicht änderbar
9010	Auftrag bereits zur Löschung vorgemerkt
9160	Auftragsidentifikation fehlt
9210	Aussetzungszeitraum zu groß
9210	Datum liegt zu weit in der Zukunft
9210	Datum liegt nicht in der Zukunft
9210	Auftrag existiert nicht, Auftragsidentifikation unbekannt
9210	Kontonummer des Auftraggebers darf nicht geändert werden

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 41

c) Bankparameterdaten

◆ Format

Name: Dauerauftrag aussetzen Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIDASS
 Bezugssegment: HKVVB
 Segmentversion: 1
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Dauerauftrag aussetzen
 Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Anzahl terminierter Aussetzungen	GD	num	1	M	1	
2	Minimale Vorlaufzeit	GD	num	..4	M	1	
3	Maximale Vorlaufzeit	GD	num	..4	M	1	
4	Aussetzungseingabe	GD	num	1	M	1	1,2,3
5	Aussetzung jährlich wiederkehrend erlaubt	GD	jn	#	M	1	

Nr. 1: Anzahl terminierter Aussetzungen

Hier ist die maximale Anzahl terminierter Aussetzungen pro Dauerauftrag einzustellen (s. auch DE „Anzahl terminierter Änderungen“, Kap. VII.1.1.4.2).

Bei einer terminierten Aussetzung kann der Kunde den Startzeitpunkt für die Aussetzung wählen. Eine nicht-terminierte Aussetzung gilt immer ab sofort.

Falls eine einzige terminierte Aussetzung erlaubt ist, überschreibt die Eingabe einer weiteren terminierten Aussetzung einen vorher eingereichten Aussetzungsauftrag.

Beispiele:

- 0: Terminierte Aussetzungen sind nicht erlaubt
- 1: Pro Dauerauftrag ist eine terminierte Aussetzung erlaubt
- 5: Pro Dauerauftrag sind 5 terminierte Aussetzungen erlaubt
- 9: keine Beschränkung

Nr. 2: Minimale Vorlaufzeit

s. Kap. „Dauerauftragseinrichtung“

Nr. 3: Maximale Vorlaufzeit

s. Kap. „Dauerauftragseinrichtung“

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 42	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

Nr. 4: Aussetzungseingabe

Es ist die Art einzustellen, in der der Kunde die Aussetzung eingeben kann.

Code	Bedeutung
1	Aussetzung erlaubt mit Angabe des Endtermins
2	Aussetzung erlaubt mit Angabe der Anzahl der Aussetzungen
3	Aussetzung erlaubt mit beiden Möglichkeiten

Nr. 5: Aussetzung jährlich wiederkehrend erlaubt

Es ist vom Kreditinstitut anzugeben, ob der Kunde auch jährlich wiederkehrende Aussetzungen (z.B. jedes Jahr von Februar bis August) eingeben darf.

◆ Beispiel

HIDASS:14:1:5+1+2+1:1:60:3:N'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 43

VII.1.1.4.4 Dauerauftragsbestand abrufen

Für jeden Dauerauftrag wird ein Segment "Dauerauftrag" als Datensegment in der Rückmeldungsnachricht übermittelt. Der Dauerauftrag wird so angezeigt, wie er zum nächsten Termin ausgeführt würde.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Dauerauftragsbestand anfordern
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HKDAB
 Bezugssegment: -
 Segmentversion: 1
 Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kontoverbindung Auftraggeber	DEG	kto	#	M	1	
3	Auftragsidentifikation	DE	an	..99	K	1	
4	Maximale Anzahl Einträge	DE	num	..4	K	1	>0
5	Aufsetzpunkt	DE	an	..35	K	1	

◆ Erläuterungen

Nr. 2: Kontoverbindung Auftraggeber

Dieses DE selektiert das Konto, zu dem die Daueraufträge angezeigt werden sollen.

Nr. 3: Auftragsidentifikation

Wird hier eine Auftragsidentifikation angegeben, wird der entsprechende Dauerauftrag angezeigt. Wird dieses Feld leer gelassen, kommen alle Daueraufträge des Kontos zur Anzeige.

Nr. 4: Maximale Anzahl Einträge

Es kann die Anzahl der rückzumeldenden Daueraufträge begrenzt werden (s. Kap. II.7.3).

Nr. 5: Aufsetzpunkt

Belegung nur zulässig, wenn vom Kreditinstitut ein Aufsetzpunkt rückgemeldet wurde (s. Kap. II.7.3).

◆ Beispiel

```
HKDAB:3:1+1234567:280:10020030+00001'
```

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 44	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

b) Kreditinstitutsrückmeldung

◆ Format

Name: Dauerauftragsbestand rückmelden
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIDAB
 Bezugssegment: HKDAB
 Segmentversion: 1
 Sender: Kreditinstitut
 Format: Dauerauftrag

◆ Belegungsrichtlinien

Nr. 10: Ausführungsdatum

Das Kreditinstitut kann das Datum der nächsten Ausführung einstellen.

Nr. 11: Auftragsidentifikation

Dieses DE enthält jeweils das vom Kreditinstitut vergebene Identifikationsmerkmal (Dauerauftragsnummer). Falls das Kreditinstitut keine Auftragsidentifikation vergibt, ist das DE nicht zu belegen.

Nr. 13: Aussetzung

Diese DEG darf nur belegt werden, wenn der Dauerauftrag zum nächsten Ausführungstermin ausgesetzt wird. In diesem Fall ist die restliche Anzahl von Aussetzungen anzuzeigen.

◆ Beispiel

```

HIDAB:3:1:5+1234567:280:10020030+7654321:280:200
30040+MEIER FRANZ++1000,:DEM+52+000+MIETE:UND NE
BENKOSTEN+19960901+00001+19960701:M:1:1:19970601
+N:::3'

HIDAB:4:1:5+1234567:280:10020030+54321:280:30040
050+SPORTVEREIN E.V.++100,:DEM+52+000+JAHRESBEIT
RAG:FÜR 1995+19960901+00002+19960101:M:12:1:1998
0101'
  
```

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
3010	Es liegen keine Einträge vor
9210	Bereichende darf nicht vor Bereichanfang liegen

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 45

c) Bankparameterdaten

◆ Format

Name: Dauerauftragsbestand Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIDABS
 Bezugssegment: HKVVB
 Segmentversion: 1
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

DEG wird nicht belegt.

◆ Beispiel

HIDABS:15:1:5+1+2'

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 46	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

VII.1.1.4.5 Dauerauftragsänderungsvormerkungen abrufen

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Dauerauftragsänderungsvormerkungen anfordern

Typ: Segment

Segmentart: Geschäftsvorfall

Kennung: HKDAA

Bezugssegment: -

Segmentversion: 1

Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kontoverbindung Auftraggeber	DEG	kto	#	M	1	
3	Auftragsidentifikation	DE	an	..99	M	1	
4	Maximale Anzahl Einträge	DE	num	..4	K	1	>0
5	Aufsetzpunkt	DE	an	..35	K	1	

◆ Erläuterungen

Nr. 2: Kontoverbindung Auftraggeber

Dieses DE selektiert das Konto, zu dem der Dauerauftrag angezeigt werden soll.

Nr. 3: Auftragsidentifikation

Es ist das Identifikationsmerkmal (Dauerauftragsnummer) des gewünschten Dauerauftrags einzustellen.

Nr. 4: Maximale Anzahl Einträge

Es kann die Anzahl der rückzumeldenden Dauerauftragsänderungen begrenzt werden (s. Kap. II.7.3).

Nr. 5: Aufsetzpunkt

Belegung nur zulässig, wenn vom Kreditinstitut ein Aufsetzpunkt rückgemeldet wurde (s. Kap. II.7.3).

◆ Beispiel

HKDAA:3:1+1234567:280:10020030+00001'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 47

b) Kreditinstitutsrückmeldung

◆ Beschreibung

Für den ausgewählten Dauerauftrag wird je **noch nicht ausgeführtem** Änderungs- bzw. Aussetzungsauftrag ein Segment "Dauerauftrag" übermittelt. Das erste Datenssegment enthält den Stand, der zum nächsten Ausführungstermin gültig ist. Liegen keine terminierten Änderungen bzw. Aussetzungen für diesen Dauerauftrag vor, werden keine weiteren Segmente gesendet.



Es bleibt dem Kreditinstitut überlassen, ob es Änderungs-/Aussetzungsaufträge oder Änderungs-/Aussetzungstermine³ zurückmeldet. D.h. zu einem Termin können u.U. mehrere Aufträge zurückgemeldet werden, von denen aber nur jeweils der letzte ausgeführt wird.

◆ Format

Name: Dauerauftragsänderungsvormerkungen rückmelden
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HIDAA
Bezugssegment: HKDAA
Segmentversion: 1
Sender: Kreditinstitut
Format: Dauerauftrag

◆ Belegungsrichtlinien

Nr. 10: Ausführungsdatum

Das DE ist für das erste Segment mit dem nächsten Ausführungsdatum und für alle weiteren Segmente jeweils mit dem Datum des Inkrafttretens der Änderung zu belegen.

◆ Beispiel

```
HIDAA:3:1:3+1234567:280:10020030+7654321:280:200
30040+MEIER FRANZ++1000,:DEM+52+000+MIETE:UND NE
BENKOSTEN+19960901+00001+19960701:M:1:1:19970601
'

HIDAA:4:1:3+1234567:280:10020030+7654321:280:200
30040+MEIER FRANZ++1100,:DEM+52+000+MIETE:UND NE
BENKOSTEN+19970101+00001+19960701:M:1:1:19970601
'
```

³ Unter Änderungs- bzw. Aussetzungstermin ist der Zeitpunkt des Inkrafttretens einer Änderung bzw. Aussetzung zu verstehen.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 48	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

◆ Ausgewählte Beispiele für Rückmeldungs-codes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
9160	Auftragsidentifikation fehlt
9210	Auftrag existiert nicht, Auftragsidentifikation unbekannt

c) Bankparameterdaten

◆ Format

Name: Dauerauftragsänderungsvormerkungen Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIDAAS
 Bezugssegment: HKVVB
 Segmentversion: 1
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

DEG wird nicht belegt.

◆ Beispiel

HIDAAS:16:1:5+1+2'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 49

VII.1.1.4.6 Dauerauftragslöschung

Löschungen gelten, sofern nichts anderes bestimmt ist, ab sofort. Darüber hinaus kann das Kreditinstitut in der BPD festlegen, ob es zusätzlich terminierte Löschungen erlaubt. Die Eingabe einer terminierten Löschung überschreibt einen evtl. vorher eingegebenen terminierten Löschauftrag.



Im Gegensatz zur Dauerauftragsänderung und -aussetzung ist eine Löschung auch möglich, wenn das Kreditinstitut keine Auftragsidentifikation für den Dauerauftrag vergibt, da im Löschauftrag die Originaldaten des Auftrags mitgeteilt werden, die dem Kreditinstitut eine eindeutige Identifizierung des Auftrags ermöglichen.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Dauerauftrag löschen
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKDAL
Bezugssegment: -
Segmentversion: 1
Sender: Kunde
Format: Dauerauftrag

◆ Belegungsrichtlinien

Es sind die gültigen Daten des Dauerauftrags einzustellen. Diese dienen zu Plausibilitätsprüfungen. Zusätzlich sind folgende Felder wie folgt zu belegen:

Nr. 10: Ausführungsdatum

Falls terminierte Löschungen erlaubt sind (s. DE „Löschung terminierbar“ in den Bankparameterdaten), ist hier das Löschedatum einzustellen. Es muß sich dabei um ein Datum handeln, zu dem eine Ausführung stattfinden würde. Ist das DE nicht eingestellt, so wird die Löschung sofort wirksam. Falls die Löschung nicht terminierbar ist, darf das DE nicht belegt werden.

Nr. 11: Auftragsidentifikation

Falls vom Kreditinstitut beim Abholen des Dauerauftragsbestands eine Auftragsidentifikation zurückgemeldet wurde, ist diese einzustellen. Ansonsten kann die Belegung entfallen.

Nr. 13: Aussetzung

Die DEG darf nicht belegt werden.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 50	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

◆ Beispiel

```
HKDAL:3:1+1234567:280:10020030+7654321:280:20030
040+MEIER FRANZ++1000,:DEM+52+000+MIETE:UND NEBE
NKOSTEN+19960901+00001+19960701:M:1:1:19970601'
```

b) Kreditinstitutsrückmeldung

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0010	Dauerauftrag zur Löschung vorgemerkt
0020	Dauerauftrag gelöscht
9010	Dauerauftrag zur Zeit nicht änderbar
9010	Dauerauftrag bereits zur Löschung vorgemerkt
9160	Auftragsidentifikation fehlt
9210	Aussetzungszeitraum zu groß
9210	Datum liegt zu weit in der Zukunft
9210	Datum liegt nicht in der Zukunft
9210	Auftrag existiert nicht, Auftragsidentifikation unbekannt
9210	Kontonummer des Auftraggebers darf nicht geändert werden
9210	Das angegebene Datum ist kein Ausführungsdatum

c) Bankparameterdaten

◆ Format

Name: Dauerauftrag löschen Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIDALS
 Bezugssegment: HKVVB
 Segmentversion: 1
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Dauerauftrag löschen
 Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Minimale Vorlaufzeit	GD	num	..4	M	1	
2	Maximale Vorlaufzeit	GD	num	..4	M	1	
3	Löschung terminierbar	GD	jn	#	M	1	

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 51

Nr. 1: Minimale Vorlaufzeit

s. Kap. „Dauerauftragseinrichtung“

Nr. 2: Maximale Vorlaufzeit

s. Kap. „Dauerauftragseinrichtung“

Nr. 3: Löschung terminierbar

Hier ist einzustellen, ob der Kunde einen Zeitpunkt für die Löschung wählen kann. Ist dies nicht der Fall, gilt die Löschung immer ab sofort.

◆ **Beispiel**

HIDALS:17:1:5+1+2+1:60:J'

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 52	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

VII.1.1.5 Einzellastschrift

Es gelten dieselben Vorschriften wie für Einzelüberweisungen. Es ist zu beachten, daß die Kontoverbindung des Empfängers durch den Zahlungspflichtigen ersetzt wird. Ebenso wird auf die von Einzelüberweisungen abweichenden Textschlüssel hingewiesen.



Zur Bearbeitung von Lastschriften ist der vorherige Abschluß einer entsprechenden Inkassovereinbarung zwischen Kunde und Kreditinstitut erforderlich, mit der der Kunde (Zahlungsempfänger) zum Lastschriftverfahren zugelassen wird und in deren Rahmen er sich verpflichtet hat, nur solche Lastschriften zum Einzug einzureichen, für die ihm eine schriftliche Einzugsermächtigung des Zahlungspflichtigen vorliegt. Sofern diese Voraussetzung nicht gegeben ist, ist dem Kunden in den UPD die Ausführung dieses Geschäftsvorfalles nicht zu gestatten.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Einzellastschrift
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKLAS
Bezugssegment: -
Segmentversion: 2
Sender: Kunde
Format: Einzelauftrag Inlandszahlungsverkehr

◆ Belegungsrichtlinien

Nr. 10: Ausführungsdatum

Die Belegung ist nicht zugelassen.

Nr. 11: Auftragsidentifikation

Die Belegung ist nicht zugelassen.

◆ Beispiel

```
HKLAS:4:2+1234567:280:10020030+7654321:280:20030
040+MEIER FRANZ++1000,:DEM+05+000+RE-NR.1234:KD-
NR.9876'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 53

b) Kreditinstitutsrückmeldung

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

◆ Ausgewählte Beispiele für RückmeldungsCodes

Es gelten die Beispiele der Einzelüberweisung. Zusätzlich können auftreten:

Code	Beispiel für Rückmeldungstext
9010	Keine Berechtigung für Lastschriftverfahren

c) Bankparameterdaten

◆ Format

Name: Lastschrift Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HILASS
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Einzelüberweisung/-lastschrift
 Typ: Datenelementgruppe
 Format: s. Einzelüberweisung

◆ Beispiel

HILASS:8:2:5+1+2+14:04:05'

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 54	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

VII.1.2 Sammelaufträge

Im Inlandszahlungsverkehr wird für Sammelaufträge das DTAUS-Format⁴ zugrundegelegt, da der Inlandszahlungsverkehr weitgehend auf dem DTAUS-Verfahren beruht.

Die kreditinstitutsseitige Prüfung erfolgt, wie in allen anderen Fällen ebenfalls, stets auf das Segment als ganzes bezogen. Enthält der Sammelauftrag Fehler, die bei der kreditinstitutsseitigen Prüfung sofort feststellbar sind, so ist das Institut berechtigt den Auftrag zurückzuweisen, sofern dem Kunden dies unmittelbar innerhalb desselben Dialoges mitgeteilt werden kann. Dies dient zur Vermeidung von Zuordnungsproblemen im Kundensystem.

Die Weiterverarbeitung des DTA-Satzes (z.B. die bankfachliche Prüfung) kann dagegen institutsindividuell gehandhabt werden. Falls dabei festgestellt wird, daß einzelne Sätze syntaktisch oder bankfachlich fehlerhaft sind, so sind diese abzulehnen, die korrekten C-Sätze jedoch zur Ausführung zu bringen (wie in den DTA-Richtlinien beschrieben). Falls hingegen festgestellt wird, daß die Konsistenz von A-, C- oder E-Satz verletzt ist (z.B. Nichtübereinstimmung der Anzahl der Aufträge oder der Summe im E-Satz mit den Beträgen der C-Sätze), so muß der komplette Sammelauftrag abgelehnt werden, unabhängig davon, ob die Einzelsätze korrekt sind.



Da die bankfachliche Korrektheit von Sammelaufträgen meist erst offline geprüft werden kann, erhält der Kunde die Information über eine eventuelle Nichtausführung im Regelfall erst über den Kontoauszug oder das Statusprotokoll. Im Statusprotokoll sollen dem Kunden die Nummern der fehlerhaften Einzelaufträge mitgeteilt werden.



Das Kundenprodukt hat vor dem Versenden eine formale Prüfung des DTA-Datensatzes gemäß DTA-Richtlinien durchzuführen (Konsistenz von A-, C- und E-Satz), damit der Datensatz ggf. kreditinstitutsseitig unmittelbar in die DTA-Verarbeitung geleitet werden kann.⁵

Eine kreditinstitutsseitige Disposition erfolgt anhand der Betragssumme des Sammelauftrags.

Die Vorgaben bezüglich der Überweisungssonderformen (vgl. Kap. VII.1.1.2) gelten in gleicher Weise auch für Sammelüberweisungen.

⁴ s. Kap. VIII.9.1

⁵ Vgl. hierzu in Kap. VIII.9.1 die Anlage „Kontrollmaßnahmen (Plausibilitäts- und Feldinhaltprüfungen)“.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 55

◆ Format

Name: Sammelauftrag Inlandszahlungsverkehr
Typ: Format

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	DTA-Datensatz	DE	bin	..	M	1	

◆ Erläuterungen

Nr. 2: DTA-Datensatz

Der DTA-Datensatz ist gemäß Spezifikation in Kap. VIII.9.1 einzustellen. Die Anzahl der maximal einzustellenden C-Sätze ergibt sich aus den Bankparameterdaten. Es ist der DTAUS0-Zeichensatz zu verwenden.

Es kommen verschiedene Versionen des DTA zur Anwendung, die anhand der HBCI-Segmentversion unterschieden werden:

Segmentversion 2:

Feld	Belegung
A 12	X'20'
C 6	Einstellung einer internen Kundennummer möglich
C 9	Betrag in DM
C 12	Belegung mit Nullen
C 17a	X'20'
E 5	Summe der DM-Beträge
E 8	Belegung mit Nullen

Segmentversion 3: (gültig ab Start der Stufe 3 der EWWU)

Feld	Belegung
A 12	Währungskennzeichen (DM/Euro)
C 6	Einstellung einer internen Kundennummer möglich
C 9	Betrag in DM
C12	Betrag in Euro
C 17a	Währungskennzeichen (DM/Euro)
E 5	Summe der DM-Beträge
E 8	Summe der Euro-Beträge

Das Kreditinstitut gibt in den Bankparameterdaten an, welches bzw. welche dieser Versionen entgegengenommen werden können.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 56	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

VII.1.2.1 Sammelüberweisung

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Sammelüberweisung
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKSUB
Bezugssegment: -
Segmentversion: 2, 3
Sender: Kunde
Format: Sammelauftrag Inlandszahlungsverkehr

◆ Belegungsrichtlinien

Nr. 2: DTA-Datensatz

Das Feld A 11b („Ausführungsdatum“) darf nicht belegt werden (Es ist mit X'20' zu füllen).

◆ Beispiel

HKSUB : 4 : 3 + @ 1 2 6 8 @ <DTAUS> '

b) Kreditinstitutsrückmeldung

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

◆ Ausgewählte Beispiele für RückmeldungsCodes

s. Einzelüberweisung. Zusätzlich gelten:

Code	Beispiel
9130	DTAUS-Format ungültig
9210	Sammelauftrag wurde abgelehnt, da Disposition fehlerhaft
9210	Ausführungsdatum hier nicht zugelassen
9220	Einzelauftrag Nr. x wurde aufgrund eines Fehlers nicht ausgeführt

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 57

c) Bankparameterdaten

◆ Format

Name: Sammelüberweisung Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HISUBS
 Bezugssegment: HKVVB
 Segmentversion: 2, 3
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Sammelüberweisung/-lastschrift
 Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Maximale Anzahl C-Sätze	GD	num	..4	M	1	
2	Maximale Anzahl Verwendungszweckzeilen	GD	num	..2	M	1	
3	Textschlüssel	GD	dig	2	M	1..n	

Nr. 1: Maximale Anzahl C-Sätze

Der Parameter gibt an, wie viele C-Sätze (Einzelüberweisungen) maximal in einen DTAUS-Sammelüberweisungsauftrag eingestellt werden dürfen. Für eine unbegrenzte Anzahl ist der Wert „0“ einzustellen.

Nr. 2: Maximale Anzahl Verwendungszweckzeilen

s. „Einzelüberweisung“

Nr. 3: Textschlüssel

s. „Einzelüberweisung“

◆ Beispiel

HISUBS:9:3:5+1+2+999:14:51:53:54'

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 58	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland

VII.1.2.2 Sammellastschrift



Analog zu Einzellastschriften ist vor der Teilnahme am Lastschriftverfahren der vorherige Abschluß einer entsprechenden Inkassovereinbarung zwischen Kunde und Kreditinstitut erforderlich.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Sammellastschrift
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HKSLA
 Bezugssegment: -
 Segmentversion: 2, 3
 Sender: Kunde
 Format: Sammelauftrag Inlandszahlungsverkehr

◆ Belegungsrichtlinien

Nr. 2: DTA-Datensatz

Das Feld A 11b („Ausführungsdatum“) darf nicht belegt werden (Es ist mit X'20' zu füllen).

◆ Beispiel

HKSLA : 4 : 3 + @ 7 6 2 @ <DTAUS> '

b) Kreditinstitutsrückmeldung

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

◆ Ausgewählte Beispiele für Rückmeldungs_codes

s. Einzelüberweisung. Zusätzlich gelten:

Code	Beispiel
9010	Keine Berechtigung für Lastschriftverfahren
9130	DTAUS-Format ungültig
9210	Sammelauftrag wurde abgelehnt, da Disposition fehlerhaft
9210	Ausführungsdatum hier nicht zugelassen
9220	Einzelauftrag Nr. x wurde aufgrund eines Fehlers nicht ausgeführt

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Inland	Stand: 02.02.1998	Seite: 59

c) Bankparameterdaten

◆ Format

Name: Sammellastschrift Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HISLAS
 Bezugssegment: HKVVB
 Segmentversion: 2, 3
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Sammelüberweisung/-lastschrift
 Typ: Datenelementgruppe
 Format: s. Sammelüberweisung

◆ Beispiel

HISLAS:10:3:5+1+2+99:14:04:05 '

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Umsatz-Informationen	Stand: 02.02.1998	Seite: 61

VII.2 Umsatz-Informationen

VII.2.1 Kontoumsätze

Kontoumsätze werden als S.W.I.F.T. MT 940 bzw. MT 942 [gemäß Spezifikation in Kapitel VIII.9.3](#) ausgestellt. Nach Fertigstellung der überarbeiteten Nutzungsrichtlinien sollen diese zur Anwendung gelangen. Auf die Verwendung des vom HBCI-Zeichensatz abweichenden SWIFT-Zeichensatzes ist zu achten.

Es kommen verschiedene Versionen der beiden S.W.I.F.T.-Formate zur Anwendung, die anhand der HBCI-Segmentversion unterschieden werden:

Altformat (Segmentversion 3):

- Im MT940 muß Feld 28 in der Form xxxxx/yy eingestellt werden. Die Verwendung von Feld 28C ist nicht zulässig.
- Im MT942 ist weder Feld 28 noch Feld 28C zulässig.
- Die Betragsfelder sind in DM einzustellen (gilt für MT 940 und 942).
- In Feld 61, Subfeld 9 kann eine Kundenreferenz bzw. 2. Bankreferenz eingestellt werden (gilt für MT 940 und 942).
- In Feld 86 können bei strukturierter Belegung die Felder 20-26 (7 Zeilen) für den Verwendungszweck genutzt werden (gilt für MT 940 und 942).
- Es können die Geschäftsvorfallcodes 085 und 086 verwendet werden. Die Verwendung der Codes 096 bis 099 ist nicht zulässig (gilt für MT 940 und 942).

Neuformat (Segmentversion 4):

- Es muß Feld 28C in der Form xxxxx/yyy eingestellt werden. Die Verwendung von Feld 28 ist nicht zulässig (gilt für MT 940 und 942).
- Die Betragsfelder sind in Kontowährung einzustellen (gilt für MT 940 und 942).
- In Feld 61, Subfeld 9 können Ursprungs- und Gebührenbetrag eingestellt werden (gilt für MT 940 und 942).
- In Feld 86 können bei strukturierter Belegung die Felder 20-29 sowie 60-63 (14 Zeilen) für den Verwendungszweck genutzt werden (gilt für MT 940 und 942).
- Es können die neuen Geschäftsvorfallcodes 096 bis 099 verwendet werden. Die Verwendung der Codes 085 und 086 ist nicht zulässig (gilt für MT 940 und 942).

Das Neuformat kann ab 01.01.1998 von den Kreditinstituten angeboten werden und wird mit dem Start der Stufe 3 der EWWU verpflichtend. Das Altformat ist gültig bis einschließlich 31.12.1998.

Das Kreditinstitut gibt in den Bankparameterdaten an, welches bzw. welche dieser Formate (Segmentversionen) verarbeitet werden können.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 62	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Umsatz-Informationen



In der Übergangsphase, in der beide Formate gültig sind, sollte ein Kundenprodukt beide Formate verarbeiten können, um multibankfähig zu sein.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Umsatz-Informationen	Stand: 02.02.1998	Seite: 63

VII.2.1.1 Kontoumsätze/Zeitraum

Realisierung Bank: verpflichtend, falls auch „Kontoumsätze/neue Umsätze“ angeboten wird, sonst optional

Realisierung Kunde: verpflichtend, falls auch „Kontoumsätze/neue Umsätze“ angeboten wird, sonst optional

a) Kundenauftrag

◆ Beschreibung

Die Lösung bietet dem Kunden die Möglichkeit, auf seinem System verlorengegangene Buchungen erneut zu erhalten.

Der maximale Zeitraum, für den rückwirkend Buchungen beim Kreditinstitut gespeichert sind, wird in den Bankparameterdaten übermittelt.

◆ Format

Name: Kontoumsätze anfordern/Zeitraum
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKKAZ
Bezugssegment: -
Segmentversion: 3, 4
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kontoverbindung Auftraggeber	DEG	kto	#	M	1	
3	Kontowährung	DE	cur	#	K	1	
4	Von Datum	DE	dat	#	K	1	
5	Bis Datum	DE	dat	#	K	1	
6	Maximale Anzahl Einträge	DE	num	..4	K	1	>0
7	Aufsetzpunkt	DE	an	..35	K	1	

◆ Erläuterungen

Nr. 2: Kontoverbindung Auftraggeber

Es ist die Kontoverbindung des Kunden anzugeben, zu der die Umsätze rückgemeldet werden sollen.

Nr. 3: Kontowährung

Falls unter einer Kontonummer verschiedene Währungskonten geführt werden, kann hier durch Angabe des ISO-Währungscode eine entsprechende Einschränkung erfolgen, um das entsprechende Konto zu identifizieren. Dieses Feld dient ausdrücklich nicht zur Bestimmung der Währung, in der die Kontoumsätze zurückgemeldet werden.

Nr. 4,5: Von Datum, Bis Datum

Durch die Eingabe eines Von- und Bis-Datums kann der Zeitraum eingegrenzt werden (s. Kap. II.7.3 „Abholauftrag“).

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 64	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Umsatz-Informationen

Nr. 6: Maximale Anzahl Einträge

Es kann die Anzahl der rückzumeldenden Buchungspositionen begrenzt werden (s. Kap. II.7.3).

Nr. 7: Aufsetzpunkt

Belegung nur zulässig, wenn vom Kreditinstitut ein Aufsetzpunkt rückgemeldet wurde (s. Kap. II.7.3).

◆ Beispiel

```
HKKAZ:3:4+1234567:280:10020030++19960701+19960730'
```

b) Kreditinstitutsrückmeldung

◆ Beschreibung

Die Online-Antwort des Kreditinstituts enthält unmittelbar die gemäß Anfragezeitraum zusammengestellten Kontoumsätze. Eine erst spätere Bereitstellung der Kontoumsätze ist wegen der dazu erforderlichen erneuten Anwahl nicht praktikabel.

Es werden stets sämtliche Umsätze der Starttages "Von Datum" in die Kontoumsätze eingestellt, auch wenn diese ganz oder teilweise mit einem vorangegangenen Auszug abgeholt wurden. Dies ermöglicht eine fehlerfreie Eliminierung von mehrfach abgeholten Buchungen durch das Kundensystem.

◆ Format

Name: Kontoumsätze rückmelden/Zeitraum
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIKAZ
 Bezugssegment: HKKAZ
 Segmentversion: 3, 4
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Gebuchte Umsätze	DE	bin	..	M	1	
3	Nicht gebuchte Umsätze	DE	bin	..	K	1	

◆ Erläuterungen

Nr. 2: Gebuchte Umsätze

Es sind die gebuchten Umsätze des Zeitraums im Format SWIFT MT 940¹ einzustellen.

¹ s. Kap. VIII.9.3.2

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Umsatz-Informationen	Stand: 02.02.1998	Seite: 65

Da jeder Buchungstag als einzelner Satz des MT 940 abgebildet wird, kann dieses DE mehrere Buchungstage umfassen. Generell sind immer komplette Buchungstage in einen MT 940-Satz einzustellen. Hiervon abweichend kann das Kreditinstitut optional in den Satz des aktuellen Tages die bis dahin gebuchten Umsätze einstellen.

Es ist der SWIFT-Zeichensatz² anzuwenden.

Nr. 3: Nicht gebuchte Umsätze

Falls vom Kreditinstitut gewünscht, können dem Kunden auch die noch nicht gebuchten Umsätze rückgemeldet werden. Diese sind im Format SWIFT MT 942³ einzustellen. Nicht gebuchte Umsätze können nicht auftreten, wenn der vom Kunden angegebene Zeitraum in der Vergangenheit liegt.

Ansonsten gelten die Anmerkungen zum DE „Gebuchte Umsätze“.

◆ Beispiel

```
HIKAZ:4:4:3+@362@<MT 940>+@102@<MT 942>'
```

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
3010	Es liegen keine Einträge vor
3040	Auftrag nur teilweise ausgeführt
9210	Bereichende darf nicht vor Bereichanfang liegen
9210	Datum muß in der Vergangenheit liegen
9210	Keine gültige Kontoverbindung des Kunden

c) Bankparameterdaten

◆ Format

Name: Kontoumsätze/Zeitraum Parameter
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HIKAZS
Bezugssegment: HKVVB
Segmentversion: 3, 4
Sender: Kreditinstitut
Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Kontoumsätze
Typ: Datenelementgruppe

² s. Kap. VIII.9.3

³ s. Kap. VIII.9.3.3

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 66	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Umsatz-Informationen

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Speicherzeitraum	GD	num	..4	M	1	>0
2	Eingabe Anzahl Einträge erlaubt	GD	jn	#	M	1	

Nr. 1: Speicherzeitraum

Der Speicherzeitraum kennzeichnet die Anzahl Tage, für die rückwirkend Umsätze vorgehalten werden, unabhängig davon, ob diese bereits abgerufen wurden oder nicht.

Nr. 2: Eingabe Anzahl Einträge erlaubt

Es ist vom Kreditinstitut anzugeben, ob die Belegung des Feldes „Maximale Anzahl Einträge“ im Kundenauftrag zugelassen ist. Falls ja, kann das Kundenprodukt die Anzahl der maximal rückzumeldenden Buchungspositionen beschränken.

◆ Beispiel

HIKAZS:11:4:5+1+2+60:J'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Umsatz-Informationen	Stand: 02.02.1998	Seite: 67

VII.2.1.2 Kontoumsätze/neue Umsätze

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Beschreibung

Das Abholen der neuen Kontoumsätze bietet gegenüber dem Abholen per Zeitraumangabe den Vorteil, daß sichergestellt ist, daß im Kundensystem Buchungen nicht doppelt erfaßt werden. Zudem wird die kreditinstitutsseitig vorzuhaltende Datenmenge minimiert. [Grundlage für die Bestimmung, welche Umsätze als 'neu' zu betrachten sind, ist stets der letzte Umsatzabruf über HBCI.](#)

Dieser Geschäftsvorfall stellt eine Übergangslösung bis zur Verfügbarkeit des HGB-konformen „Elektronischen Kontoauszug“ dar.

Der maximale Zeitraum, für den rückwirkend Buchungen beim Kreditinstitut gespeichert sind, wird in den Bankparameterdaten übermittelt.

◆ Format

Name: Kontoumsätze anfordern/neue Umsätze
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKKAN
Bezugssegment: -
Segmentversion: 3, 4
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kontoverbindung Auftraggeber	DEG	kto	#	M	1	
3	Kontowährung	DE	cur	#	K	1	
4	Maximale Anzahl Einträge	DE	num	..4	K	1	>0
5	Aufsetzpunkt	DE	an	..35	K	1	

◆ Erläuterungen

Nr. 2: Kontoverbindung Auftraggeber

Es ist die Kontoverbindung des Kunden anzugeben, zu der die Umsätze rückgemeldet werden sollen.

Nr. 3: [Kontowährung](#)

Falls unter einer Kontonummer verschiedene Währungskonten geführt werden, kann hier durch Angabe des ISO-Währungscode eine entsprechende Einschränkung erfolgen, um das entsprechende Konto zu identifizieren. Dieses Feld dient ausdrücklich nicht zur Bestimmung der Währung, in der die Kontoumsätze zurückgemeldet werden.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 68	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Umsatz-Informationen

Nr. 4: Maximale Anzahl Einträge

Es kann die Anzahl der rückzumeldenden Buchungspositionen begrenzt werden (s. Kap. II.7.3).

Nr. 5: Aufsetzpunkt

Belegung nur zulässig, wenn vom Kreditinstitut ein Aufsetzpunkt rückgemeldet wurde (s. Kap. II.7.3).

♦ Beispiel

HKKAN: 3: 4+1234567: 280: 10020030 '

b) Kreditinstitutsrückmeldung

♦ Format

Name: Kontoumsätze rückmelden/neue Umsätze
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HIKAN
Bezugssegment: HKKAN
Segmentversion: 3, 4
Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Gebuchte Umsätze	DE	bin	..	M	1	
3	Nicht gebuchte Umsätze	DE	bin	..	K	1	

♦ Erläuterungen

s. „Kontoumsätze rückmelden/Zeitraum“

♦ Beispiel

HIKAN: 4: 4: 3+@362@<MT 940>+@102@<MT 942> '

♦ Ausgewählte Beispiele für Rückmeldungs-codes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
3010	Es liegen keine Einträge vor
3040	Auftrag nur teilweise ausgeführt
9210	Keine gültige Kontoverbindung des Kunden

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Umsatz-Informationen	Stand: 02.02.1998	Seite: 69

c) Bankparameterdaten

◆ Format

Name: Kontoumsätze/neu Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIKANS
 Bezugssegment: HKVVB
 Segmentversion: 3, 4
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Kontoumsätze
 Typ: Datenelementgruppe
 Format: s. „Kontoumsätze abholen/Zeitraum“

◆ Beispiel

HIKANS:12:4:5+1+2+60:J'

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 70	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Umsatz-Informationen

VII.2.2 Saldenabfrage

Die Saldenabfrage liefert für das angegebene Konto bzw. für alle Konten des Kunden den aktuellen Saldo sowie weitere Saldeninformationen zurück.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Saldenabfrage
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HKSAL
 Bezugssegment: -
 Segmentversion: 3
 Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kontoverbindung Auftraggeber	DEG	kto	#	M	1	
3	Alle Konten	DE	jn	#	M	1	
4	Kontowährung	DE	cur	#	K	1	
5	Maximale Anzahl Einträge	DE	num	..4	K	1	>0
6	Aufsetzpunkt	DE	an	..35	K	1	

◆ Erläuterungen

Nr. 2: Kontoverbindung Auftraggeber

Es ist diejenige Kontoverbindung des Kunden einzustellen, für die der Saldo angefragt wird. Wählt der Kunde die Option „Alle Konten“, so ist eine beliebige gültige Kontoverbindung des Kunden einzustellen.

Nr. 3: Alle Konten

Mit dieser Option kann gewählt werden, ob der Saldo nur des angegebenen Kontos oder aller Konten des Kunden, für die er eine Zugriffsberechtigung besitzt und für die ein Saldo angegeben werden kann, rückgemeldet werden soll.



Mit Hilfe der Option „Alle Konten“ kann im Kundenprodukt ein Finanzstatus des Kunden (Überblick über alle Geld- und Finanzanlagen) realisiert werden. Zu diesem Finanzstatus zählen jedoch nur diejenigen Konten, die im Kreditinstitut für diesen Kunden geführt werden und zu denen ein Saldo angegeben werden kann. In der Praxis zählen jedoch oftmals bestimmte Konten für den Kunden nicht zum Finanzstatus (z.B. Konten, für die der Kunde lediglich bevollmächtigt ist), andere fehlen jedoch, wie z.B. Konten zu denen kein Saldo

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Umsatz-Informationen	Stand: 02.02.1998	Seite: 71

existiert (Wertpapierkonten) oder Konten, die bei anderen Instituten geführt werden.

In diesem Fall kann der Finanzstatus vom Kundenprodukt durch Hintereinanderschaltung mehrerer Saldenabfragen zu jeweils einzelnen Konten erzeugt werden. Dieser Finanzstatus kann auch Konten verschiedener Kreditinstitute umfassen, indem mehrere HBCI-Dialoge mit verschiedenen Instituten automatisch nacheinander durchgeführt werden.

Nr. 4: Kontowährung

Falls unter einer Kontonummer verschiedene Währungskonten geführt werden, kann hier durch Angabe des ISO-Währungscode eine entsprechende Einschränkung erfolgen, um das entsprechende Konto zu identifizieren. Dieses Feld dient ausdrücklich nicht zur Bestimmung der Währung, in der die Salden zurückgemeldet werden.

Nr. 5: Maximale Anzahl Einträge

Es kann die Anzahl der rückzumeldenden Konten begrenzt werden (s. Kap. II.7.3).

Nr. 6: Aufsetzpunkt

Belegung nur zulässig, wenn vom Kreditinstitut ein Aufsetzpunkt rückgemeldet wurde (s. Kap. II.7.3).

◆ Beispiel

HKSAL:3:3+1234567:280:10020030+N'

b) Kreditinstitutsrückmeldung

◆ Beschreibung

Das Kreditinstitut hat in jedem Fall den „gebuchten Saldo“ zurückzumelden. Falls im Kreditinstitut verfügbar, können auch die anderen Kontoinformationen rückgemeldet werden. Die Währung, in der die Beträge rückgemeldet werden, entspricht stets der Kontenwährung.

Falls der Kunde „Alle Konten“ gewählt hat, ist das Segment „Saldenrückmeldung“ für jedes Konto jeweils einmal einzustellen.

◆ Format

Name: Saldenrückmeldung
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HISAL
Bezugssegment: HKSAL
Segmentversion: 3
Sender: Kreditinstitut

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 72	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Umsatz-Informationen

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kontoverbindung Auftraggeber	DEG	kto	#	M	1	
3	Kontoproduktbezeichnung	DE	an	..30	M	1	
4	Kontowährung	DE	cur	#	M	1	
5	Gebuchter Saldo	DEG	sdo	#	M	1	
6	Saldo der vorgemerkten Umsätze	DEG	sdo	#	K	1	
7	Kreditlinie	DEG	btg	#	K	1	
8	Verfügbarer Betrag	DEG	btg	#	K	1	
9	Bereits verfügbarer Betrag	DEG	btg	#	K	1	

♦ Erläuterungen

Nr. 3: Kontoproduktbezeichnung

Es ist die Produktbezeichnung des Kontos einzustellen. Diese Bezeichnung ist vom Kreditinstitut frei wählbar.

Nr. 4: Kontowährung

Es ist die Währung des betreffenden Kontos anzugeben. Falls unter einer Kontonummer verschiedene Währungskonten geführt werden, dient dieses Feld zur Differenzierung.

Nr. 5: Gebuchter Saldo

Saldo, der nur bereits gebuchte Positionen berücksichtigt, nicht jedoch in der Schwebe befindliche Posten.

Nr. 6: Saldo der vorgemerkten Umsätze

Es ist der Saldo der noch nicht verbuchten Umsätze einzustellen.

Nr. 7: Kreditlinie

Kontokorrentkredit. Die Ermittlung der Kreditlinie kann institutsspezifisch differieren.

Nr. 8: Verfügbarer Betrag

Es ist der Betrag einzustellen, der im Augenblick der Saldenrückmeldung für den Kunden maximal disponiert werden kann. Die Ermittlung des verfügbaren Betrags kann institutsspezifisch differieren.

Nr. 9: Bereits verfügbarer Betrag

Es ist der Betrag einzustellen, über den der Kunde im Augenblick der Saldenrückmeldung bereits verfügt hat. Die Ermittlung des bereits verfügbaren Betrags kann institutsspezifisch differieren.



Die vom Kreditinstitut übermittelten Daten kann das Kundenprodukt dazu verwenden, dem Kunden beliebige abgeleitete Informationen zu seinem Konto (z.B. Disposaldo, offener Saldo, Verfügungsrahmen, Limit) zu errechnen und zur Verfügung zu stellen.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Umsatz-Informationen	Stand: 02.02.1998	Seite: 73

◆ Beispiel

```
HISAL:4:3:3+1234567:280:10020030+Giro Spezial+DE
M+C:1000,:DEM:19960701+D:500,:DEM:19960701+5000,
:DEM+7138,35:DEM+1476,98:DEM'
```

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
3040	Auftrag nur teilweise ausgeführt
9210	Keine gültige Kontoverbindung des Kunden
9210	Konto hat keinen Saldo, da Depotkonto

c) Bankparameterdaten

◆ Format

Name: Saldenabfrage Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HISALS
 Bezugssegment: HKVVB
 Segmentversion: 3
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Die DEG wird nicht belegt.

◆ Beispiel

```
HISALS:13:3:5+1+2'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen	Stand: 02.02.1998	Seite: 75

VII.3 Termineinlagen

Derzeit ist nur die Festgeldanlage vorgesehen. Die Anlage von Kündigungsgeldern ist nicht möglich.

Für die Festgeldanlage sind die folgenden Geschäftsvorfälle vorgesehen:

- Abfrage der z.Zt. gültigen Konditionen
- Auftrag zur Neuanlage eines Festgeldes
- Ändern vorhandener Festgelder
- Prolongation bestehender Festgeldanlagen
- Anzeige des Festgeldbestandes eines Kunden
- Widerruf einer vorgemerkten Festgeldneuanlage
- Widerruf einer Festgeldprolongation

Der Abruf von Umsätzen (Nachträgen) ist per HBCI nicht vorgesehen.

Die Abbildung zeigt die Abfolge der Geschäftsvorfälle:

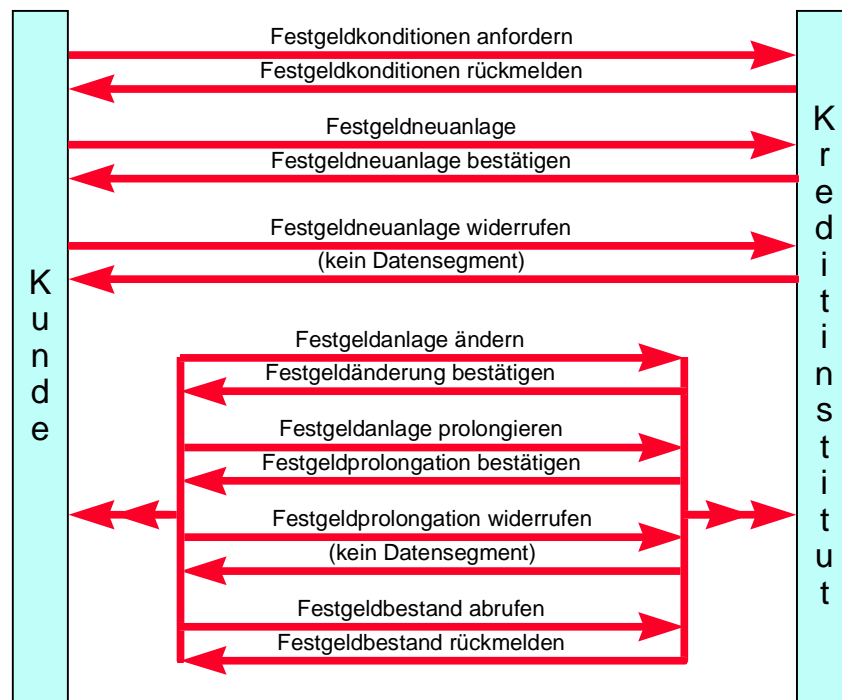


Abb. 21: Lebenszyklus Festgeld

Im Rahmen der Festgeldanlage werden verschiedene Konten spezifiziert (Anlagekonto, Belastungskonto etc.). Welches dieser Konten jeweils zur Berechtigungsprüfung herangezogen wird, kann kreditinstitutsindividuell entschieden werden.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 76	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen

Folgende Datenformate sind für die Festgeldanlage vorgesehen.

◆ Format

Name: Festgeld

Typ: Format

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Anlagekonto	DEG	kto	#	K	1	
3	Kontraktreferenz	DE	id	#	K	1	
4	Anlagebetrag	DEG	btg	#	M	1	
5	Festgeldkondition	DEG			M	1	
6	Belastungskonto	DEG	kto	#	M	1	
7	Eigene Rechnung	DE	jn	#	M	1	
8	Wiederanlagekennzeichen	DE	num	1	M	1	1,2
9	Kontoauszugkennzeichen	DE	num	1	K	1	1,2
10	Ausbuchungskonto	DEG	kto	#	K	1	
11	Zinsgutschriftkonto	DEG	kto	#	K	1	
12	Version der Konditionen	DEG			K	1	
13	Zinsertrag voraussichtlich	DEG	btg	#	K	1	
14	Festgeldstatus	DE	num	1	K	1	
15	Prolongation	DEG			K	1	

Nr. 2: Anlagekonto

Kontonummer des Festgeldkontos

Nr. 3: Kontraktreferenz

Dieses DE kann als zusätzliches Identifikationsmerkmal für die Festgeldanlage dienen, wenn bspw. auf einem Anlagekonto mehrere Festgelder angelegt werden können.

Nr. 4: Anlagebetrag

Betrag, auf den die Festgeldanlage lautet

Nr. 5: Festgeldkondition

Format: s.u.

Nr. 6: Belastungskonto

Es ist das Kontokorrentkonto des Kunden einzustellen, auf dem die Belastung des Anlagebetrages erfolgt. Das Belastungskonto muß bei demselben Kreditinstitut wie das Anlagekonto geführt werden.

Nr. 7: Eigene Rechnung

Es ist anzugeben, ob der Kunde bei der Festgeldanlage auf eigene oder auf fremde Rechnung handelt (Diese Angabe ist im Rahmen des Geldwäschegesetzes relevant). Wird hier mit „Nein“ (d.h. fremde Rechnung) geantwortet, ist i.d.R. eine manuelle Nachbearbeitung des Auftrags im Institut notwendig.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen	Stand: 02.02.1998	Seite: 77



Das Kundenprodukt sollte in der Eingabemaske die folgende Formulierung verwenden:

Der/Die Kontoinhaber handelt/handeln für eigene Rechnung:

☐ ja ☐ nein

Nr. 8: Wiederanlagekennzeichen

Das Wiederanlagekennzeichen gibt an, wie die Festgeldanlage bei ihrer Fälligkeit behandelt wird.

Code	Bedeutung
1	ausbuchen
2	um den vereinbarten Zeitraum prolongieren

Nr. 9: Kontoauszugkennzeichen

Falls das Kreditinstitut mehrere Möglichkeiten für die Zustellung des Kontoauszugs vorsieht (s. Angaben in den BPD), kann der Kunde wählen, wie der Kontoauszug zugestellt werden soll.

Nr. 10: Ausbuchungskonto

Gibt an, welchem Konto bei Fälligkeit der Anlage der Ausbuchungsbetrag gutgeschrieben werden soll.

Nr. 11: Zinsgutschriftkonto

Gibt an, welchem Konto die Anlagezinsen gutgeschrieben werden sollen.

Nr. 12: Version der Konditionen

Format: s.u.

Nr. 13: Zinsertrag voraussichtlich

Erwarteter Zinsertrag der laufenden Anlageperiode.



Der Kunde ist darauf hinzuweisen, daß diese Angabe nicht rechtsverbindlich ist.

Nr. 14: Festgeldstatus

Der Festgeldstatus beschreibt den Status der Anlage.

Code	Bedeutung
1	aktiv
2	vorgemerkt

Nr. 15: Prolongation

Format: s.u.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 78	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen

◆ Format

Name: Festgeldkondition
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Anlagedatum	GD	dat	#	M	1	
2	Ablaufdatum	GD	dat	#	M	1	
3	Zinssatz	GD	wrt	#	M	1	
4	Zinsmethode	GD	an	1	M	1	
5	Anlagebetrag von	GDG	btg	#	M	1	
6	Anlagebetrag bis	GDG	btg	#	K	1	
7	Konditionenidentifikation	GD	id	#	K	1	
8	Konditionenbezeichnung	GD	an	..30	K	1	

Nr. 1: Anlagedatum

Startzeitpunkt der Anlage. Es ist das Datum einzustellen, zu dem der Abschluß und die Valutierung der Festgeldanlage erfolgt, wenn der Anlageauftrag zu diesem Zeitpunkt im Kreditinstitut eingehen würde. Nicht-Buchungstage sind hierbei zu berücksichtigen.

Die Laufzeit, die sich aus Anlage- und Ablaufdatum errechnet, hat dabei mit der in den Festgeldkonditionen vorgegebenen Zinsmethode zu korrespondieren.

Nr. 2: Ablaufdatum

Endzeitpunkt der Anlage.



Das Kundenprodukt sollte aus Anlage- und Ablaufdatum die Laufzeit der Anlage berechnen, da dies dem Kunden i.d.R. einen besseren Vergleich ermöglicht.

Nr. 3: Zinssatz

Zinssatz der Anlage p.a. (Die Anzahl der Nachkommastellen ist kreditinstitutsspezifisch).

Nr. 4: Zinsmethode

Es ist die dem Zinssatz zugrunde liegende Zinsmethode anzugeben (Codierung gemäß SWIFT).

Code	Bedeutung	
	Monat	Jahr
A	30 Tage	360 Tage
B	28-31 Tage	360 Tage
C	28-31 Tage	365/6 Tage
D	30 Tage	365/6 Tage
E	28-31 Tage	365 Tage
F	30 Tage	365 Tage

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen	Stand: 02.02.1998	Seite: 79

Nr. 5: Anlagebetrag von

Es ist die Untergrenze des jeweiligen Betragsintervalls anzugeben. Der jeweils niedrigste angegebene Betragswert zu einer Laufzeit stellt den Mindestanlagebetrag dar.

Bei einem nach oben offenen Intervall ist keine Obergrenze anzugeben.

Nr. 6: Anlagebetrag bis

Es ist die Obergrenze des jeweiligen Betragsintervalls anzugeben. Bei einem nach oben offenen Intervall ist das DE nicht zu belegen.

Nr. 7: Konditionenidentifikation

Optional kann eine Identifikation mitgeteilt werden, die die jeweilige Kondition eindeutig kennzeichnet.

Nr. 8: Konditionenbezeichnung

Es kann optional ein Name für die Kondition bzw. die Festgeldanlage angegeben werden.

◆ **Format**

Name: Version der Konditionen
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Konditionenversion	GD	an	..10	M	1	
2	Datum der Übermittlung	GD	dat	#	M	1	
3	Uhrzeit der Übermittlung	GD	tim	#	M	1	

Nr. 1: Konditionenversion

Bei jeder Änderung der Festgeldkonditionen ist die Version kreditinstitutsseitig zu aktualisieren. Die Art der Versionsverwaltung (Versionsnummer oder Versionsdatum) kann vom Kreditinstitut frei gewählt werden. Falls keine Versionsverwaltung geführt wird, ist das aktuelle Tagesdatum einzustellen.

Nr. 2: Datum der Übermittlung

Es ist das Datum der Übermittlung der Konditionen einzustellen. Diese Angabe wird bei einem Auftrag zur Festgeldanlage zurückgemeldet und dient kreditinstitutsseitig zu Informationszwecken.

Nr. 3: Uhrzeit der Übermittlung

Es ist die Uhrzeit der Übermittlung der Konditionen einzustellen. Diese Angabe wird bei einem Auftrag zur Festgeldanlage zurückgemeldet und dient kreditinstitutsseitig zu Informationszwecken.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 80	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen

◆ Format

Name: Prolongation
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Prolongationslaufzeit	GD	num	..3	M	1	
2	Anlagebetrag neu	GDG	btg	#	M	1	
3	Wiederanlagekennzeichen bei Prolongation	GD	num	1	M	1	1,2

Nr. 1: Prolongationslaufzeit

Es darf nur eine gemäß der Konditionen zulässige Laufzeit gewählt werden.

Nr. 2: Anlagebetrag neu

Betrag, der für die nächste Anlageperiode gültig sein soll. Bei einer Erhöhung des Anlagebetrages wird das bei der Festgeldneuanlage angegebene Belastungskonto bzw. bei einer Verminderung das Ausbuchungskonto herangezogen.

Nr. 3: Wiederanlagekennzeichen bei Prolongation

s. DE „Wiederanlagekennzeichen“

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen	Stand: 02.02.1998	Seite: 81

VII.3.1 Festgeldkonditionen



Die abgerufenen Festgeldkonditionen können dem Kundenprodukt auch dazu dienen, Modell- oder Beispielrechnungen im Offline-Betrieb auf der Basis aktueller Daten durchzuführen.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Beschreibung

Die Standardkonditionen werden betrags- und laufzeitabhängig ermittelt.

◆ Format

Name: Festgeldkonditionen anfordern
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKFGK
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Währung der Konditionen	DE	cur	#	M	1	
3	Maximale Anzahl Einträge	DE	num	..4	K	1	>0
4	Aufsetzpunkt	DE	an	..35	K	1	

◆ Erläuterungen

Nr. 2: Währung der Konditionen

Der Kunde hat anzugeben, in welcher Währung die Festgeldanlagen geführt werden sollen, zu denen er die Konditionen abrufen möchte. Die gültigen Währungskennzeichen stellt das Kreditinstitut in die Bankparameterdaten ein.

Nr. 3: Maximale Anzahl Einträge

Es kann die Anzahl der rückzumeldenden Konditionen begrenzt werden (s. Kap. II.7.3).

Nr. 4: Aufsetzpunkt

Belegung nur zulässig, wenn vom Kreditinstitut ein Aufsetzpunkt rückgemeldet wurde (s. Kap. II.7.3).

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 82	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen

◆ Beispiel

HKFGK : 3 : 1 + DEM '

b) Kreditinstitutsrückmeldung

◆ Format

Name: Festgeldkonditionen rückmelden
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HIFGK
Bezugssegment: HKFGK
Segmentversion: 1
Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Version der Konditionen	DEG			M	1	
3	Festgeldkondition	DEG			M	1..99	

◆ Beispiel

HIFGK:3:1:3+38516:19960701:152245+19960701:19960731:3,:A:10000,:DEM:19999,:DEM:1:30 Tage, 3%+19960701:19960731:3,125:A:20000,:DEM:29999,:DEM:2:30 Tage, 3,125%+19960701:19960731:3,25:A:30000,:DEM::3:30 Tage, 3,25%+19960701:19960831:3,25:A:10000,:DEM:19999,:DEM:4:60 Tage, 3,25%+19960701:19960831:3,375:A:20000,:DEM:29999,:DEM:5:60 Tage, 3,375%+19960701:19960831:3,5:A:30000,:DEM::6:60 Tage, 3,5%+19960701:19960930:3,5:A:10000,:DEM:19999,:DEM:7:90 Tage, 3,5%+19960701:19960930:3,75:A:20000,:DEM:29999,:DEM:8:90 Tage, 3,75%+19960701:19960930:3,875:A:30000,:DEM::9:90 Tage, 3,875%'

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
3010	Information wird zur Zeit nicht angeboten

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen	Stand: 02.02.1998	Seite: 83

c) Bankparameterdaten

◆ Format

Name: Festgeldkonditionen Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIFGKS
 Bezugssegment: HKVVB
 Segmentversion: 1
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Festgeldkonditionen
 Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Währung der Konditionen	GD	cur	#	M	1-99	

◆ Erläuterungen

Nr. 1: Währung der Konditionen

Es sind diejenigen Währungen anzugeben, in denen das Kreditinstitut Festgeldkonditionen zurückmelden kann.

◆ Beispiel

HIFGKS:26:1:5+1+2+DEM:CHF:FRF '

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 84	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen

VII.3.2 Festgeldneuanlage

Ein Auftrag zur Festgeldanlage bedingt im Regelfall die Eröffnung eines Festgeldkontos. Da mit einer Kontoeröffnung üblicherweise administrative Vorgänge (z.B. Bonitätsprüfung) verbunden sind, deren Umfang einerseits davon abhängig ist, ob der Kunde bereits ein Konto beim betreffenden Institut führt, und andererseits davon abhängt, inwieweit diese Vorgänge einer manuellen Bearbeitung bedürfen, ist die kreditinstitutsseitige Reaktion auf einen Auftrag zur Festgeldanlage institutsindividuell verschieden. Eine weitgehend problemlose Bearbeitung des Auftrags ist insbesondere dann möglich, wenn der dialogführende Kunde Inhaber des Belastungskontos ist. Eine Festgeldanlage zugunsten Dritter per HBCI ist nicht vorgesehen. Die Frage, auf welchen Namen ein Festgeldkonto eröffnet werden soll, ist rein bankfachlicher Natur und somit nicht Aufgabe der Schnittstelle, sondern des Kreditinstituts.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Beschreibung



Änderungen der Festgeldkonditionen können sehr kurzfristig erfolgen. Daher hat der Kunde vor der Versendung eines Festgeldauftrages die aktuellen Konditionen abzurufen (s.o.). Falls der Kunde im Besitz eines veralteten Konditionsbestandes ist, kann der Auftrag abgewiesen werden.

◆ Format

Name: Festgeldneuanlage
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKFGN
Bezugssegment: -
Segmentversion: 2
Sender: Kunde
Format: Festgeld

◆ Belegungsrichtlinien

Nr. 2: Anlagekonto

Belegung nicht zulässig.

Nr. 3: Kontraktreferenz

Belegung nicht zulässig.

Nr. 4: Anlagebetrag

Der Kunde hat den gewünschten Anlagebetrag anzugeben. Dieser muß größer oder gleich dem in den Festgeldkonditionen mitgeteilten Mindestanlagebetrag sein.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen	Stand: 02.02.1998	Seite: 85

Nr. 5: Festgeldkondition

Es ist die Festgeldkondition anzugeben, zu der der Kunde den Vertrag abschließen möchte. Die Kondition ist so einzustellen, wie sie vom Kreditinstitut beim Abruf der Konditionen übermittelt wurde. Insbesondere ist die Konditionenidentifikation anzugeben, sofern sie vom Kreditinstitut mitgeteilt wurde.

Falls die Angaben in den Konditionen inkonsistent sind oder die Konditionen nicht mehr aktuell sind, kann der Auftrag abgelehnt werden.

Nr. 10: Ausbuchungskonto

Falls als Ausbuchungskonto das Belastungskonto gewünscht wird, braucht das Feld nicht belegt werden. Eine vom Belastungskonto abweichende Belegung ist nur erlaubt, falls laut BPD zugelassen.

Nr. 11: Zinsgutschriftkonto

Falls die Zinsen kapitalisiert (d.h. am Ende der Anlageperiode dem Anlagekonto gutgeschrieben) werden sollen, darf das Feld nicht belegt werden. Falls statt dessen die Auszahlung der Zinsen gewünscht wird, ist zu prüfen, ob laut BPD ein abweichendes Zinsgutschriftkonto erlaubt ist. Wenn ja, kann ein beliebiges Zinsgutschriftkonto eingestellt werden. Wenn nicht, ist das Belastungskonto einzustellen.

Nr. 12: Version der Konditionen

Das DE muß belegt werden. Es ist die Version der aktuellen Festgeldkonditionen einzustellen, die der Kunde mit dem Auftrag „Festgeldkonditionen abfragen“ erhält. Diese Version dient der Plausibilitätsprüfung, falls die vom Kunden übermittelte Anlagekondition ungültig ist.

Nr. 13: Zinsertrag voraussichtlich

Belegung nicht zulässig.

Nr. 14: Festgeldstatus

Belegung nicht zulässig.

Nr. 15: Prolongation

Belegung nicht zulässig.

♦ Beispiel

```
HKFGN:3:2++10000,:DEM+19960701:19960831:3,25:A:
10000,:DEM:19999,:DEM:4:60 Tage, 3,25%+1234567:2
80:10020030+J+1+1+1234567:280:10020030++38516:19
960701:152245'
```

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 86	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen

b) Kreditinstitutsrückmeldung

◆ Format

Name: Festgeldneuanlage bestätigen
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIFGN
 Bezugssegment: HKFGN
 Segmentversion: 2
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Anlagekonto	DEG	kto	#	K	1	
3	Kontraktreferenz	DE	id	#	K	1	

◆ Erläuterungen

Nr. 2: Anlagekonto



Falls das Kreditinstitut schon bei der Einreichung das Anlagekonto zurückmelden kann, sollte diese Möglichkeit genutzt werden.

Andernfalls muß das Kundensystem nach einer Festgeldneuanlage zunächst die betreffende Anlagekontonummer in Erfahrung bringen, bevor der Kunde eine Modifikation seiner Anlage (Änderung, Prolongation) vornehmen kann. Hierzu ist zunächst ein Abruf des gesamten Festgeldbestandes (s. Kap. VII.3.5) vorzunehmen, wobei das DE „Alle Konten“ auf 'J' gesetzt ist. In der Antwortnachricht wird dem Kunden für jede Anlage die entsprechende Anlagekontonummer zurückgemeldet.

Nr. 3: Kontraktreferenz

s. Nr. 2 „Anlagekonto“

◆ Beispiel

HIFGN: 3: 2: 3+7654321: 280: 10020030+123 '

◆ Ausgewählte Beispiele für Rückmeldungs-codes

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
0020	Auftrag ausgeführt
9210	Festgeldkonditionen sind nicht aktuell; bitte erst aktualisieren
9210	Betrag zu niedrig
9210	Kontonummer existiert nicht
9210	Keine gültige Kontonummer des Kunden

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen	Stand: 02.02.1998	Seite: 87

c) Bankparameterdaten

◆ Format

Name: Festgeldneuanlage Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIFGNS
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Festgeldneuanlage
 Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Abweichendes Ausbuchungskonto erlaubt	GD	jn	#	M	1	
2	Abweichendes Zinsgutschriftkonto erlaubt	GD	jn	#	M	1	
3	Kontoauszugkennzeichen	GD	num	1	K	1..9	1,2

Nr. 3: Kontoauszugkennzeichen

Es sind die kreditinstitutsseitig zugelassenen Möglichkeiten für die Zustellung des Kontoauszugs anhand der nachfolgenden Codes anzugeben:

Code	Bedeutung
1	Postzustellung
2	Abholung (z.B. Kontoauszugdrucker)

◆ Beispiel

HIFGNS : 27 : 2 : 5+1+2+J : J : 1 '

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 88	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen

VII.3.3 Festgeldänderung

Mit Hilfe der Festgeldänderung können Änderungen für bestehende Festgeldanlagen während der Laufzeit durchgeführt werden. Betrags- und Laufzeitänderungen sind nicht zugelassen. Die Änderungen werden sofort wirksam. Es können nur aktive Festgeldanlagen geändert werden. Die Änderung von vorgemerkten Anlagen ist nicht möglich.

Welche Daten änderbar sind, bestimmt das Kreditinstitut in den Bankparameterdaten. Grundsätzlich änderbar sind die folgenden Daten:

- Wiederanlagekennzeichen
- Kontoauszugkennzeichen
- Ausbuchungskonto
- Zinsgutschriftkonto

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Festgeldanlage ändern
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HKFGA
 Bezugssegment: -
 Segmentversion: 2
 Sender: Kunde
 Format: Festgeld

◆ Belegungsrichtlinien

Nr. 2: Anlagekonto

Es ist die Nummer des zu ändernden Festgeldkontos anzugeben.

Nr. 3: Kontraktreferenz

Sofern eine Kontraktreferenz erteilt wurde, ist diese anzugeben.

Nr. 4-7:

Es sind die gültigen Daten der Festgeldanlage einzustellen. Diese dienen zu Plausibilitätsprüfungen.

Nr. 8-11:

Für alle laut Bankparameterdaten änderbaren Felder sind die neuen Werte einzustellen, d.h. für die Felder, die änderbar sind, jedoch nicht geändert werden sollen, sind die bisherigen Werte einzutragen. Dies ist erforderlich, um ein Feld auf 'nicht belegt' ändern zu können (bspw. erforderlich beim Zinsgutschriftkonto).

Nr. 12-15:

Belegung nicht zulässig.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen	Stand: 02.02.1998	Seite: 89

◆ Beispiel

```
HKFGA:4:2+7654321:280:10020030+123+10000,:DEM+19
960701:19960831:3,25:A:10000,:DEM:19999,:DEM:4:6
0 Tage, 3,25%+1234567:280:10020030+J+2+1+1234567
:280:10020030'
```

b) Kreditinstitutsrückmeldung

◆ Format

Name: Festgeldänderung bestätigen
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIFGA
 Bezugssegment: HKFGA
 Segmentversion: 2
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Anlagekonto	DEG	kto	#	M	1	
3	Kontraktreferenz	DE	id	#	K	1	
4	Anlagekonto alt	DEG	kto	#	K	1	
5	Kontraktreferenz alt	DE	id	#	K	1	

◆ Erläuterungen

Nr. 2: Anlagekonto

Es ist die für diese Festgeldanlage aktuell gültige Anlagekontonummer anzugeben.

Nr. 3: Kontraktreferenz

s. Nr. 2 „Anlagekonto“

Nr. 4: Anlagekonto alt

In der Regel wird die Anlagekontonummer durch einen Änderungsauftrag nicht modifiziert. Dies ist jedoch möglich, wenn z.B. die Änderung bankseitig durch eine Löschung und Neueinreichung realisiert wird. In diesem Fall muß dem Kundensystem die neu vergebene und aus Zuordnungsgründen die bisherige Anlagekontonummer mitgeteilt werden. Falls keine Änderung der Anlagekontonummer stattgefunden hat, ist das DE nicht zu belegen.



Falls eine neue Anlagekontonummer vergeben wurde, ist der lokale Bestand im Kundenprodukt zu aktualisieren.

Nr. 5: Kontraktreferenz alt

s. Nr. 4 „Anlagekonto alt“

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 90	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen

◆ Beispiel

HIFGA:3:2:3+7654322:280:10020030+124+7654321:280
:10020030+123'

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
0020	Festgeldanlage geändert
9210	Festgeldkonto existiert nicht
9210	Konto ist kein Festgeldkonto
9210	Keine gültige Kontonummer des Kunden

c) Bankparameterdaten

◆ Format

Name: Festgeld ändern Parameter
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HIFGAS
Bezugssegment: HKVVB
Segmentversion: 2
Sender: Kreditinstitut
Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Festgeld ändern
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Wiederanlagekennzeichen änderbar	GD	jn	#	M	1	
2	Kontoauszugkennzeichen änderbar	GD	jn	#	M	1	
3	Ausbuchungskonto änderbar	GD	jn	#	M	1	
4	Zinsgutschriftkonto änderbar	GD	jn	#	M	1	

Nr. 1-4:

Es ist jeweils einzustellen, ob das betreffende Feld durch den Kunden änderbar ist.

◆ Beispiel

HIFGAS:28:2:5+1+2+J:J:J:N'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen	Stand: 02.02.1998	Seite: 91

VII.3.4 Festgeldprolongation

Mit Hilfe der Prolongation sind Änderungen einer bestehenden Festgeldanlage für die nächste Anlageperiode möglich. Eine Prolongation kann nur für eine bereits bestehende Festgeldanlage durchgeführt werden. Die Rahmendaten der Anlage (z.B. Belastungskonto) werden bei der Neuanlage festgelegt und können im Rahmen der Prolongation nicht verändert werden.

Falls bei der Festgeldneuanlage mit Hilfe des Wiederanlagekennzeichens festgelegt wurde, daß die Anlage bei ihrer Fälligkeit prolongiert werden soll, ist keine explizite Prolongation erforderlich. Ein Prolongationsauftrag ist vom Kunden lediglich dann zu senden, wenn:

- die bei der Neuanlage getroffene Entscheidung, daß die Anlage nach ihrer Fälligkeit ausgebucht werden soll, revidiert werden soll (In diesem Fall wird das bei der Neuanlage festgelegte Wiederanlagekennzeichen überschrieben).
- für den nächsten Anlagezeitraum die Laufzeit oder der Anlagebetrag geändert werden soll.



Prolongation bedeutet nicht zwingend, daß die in der aktuellen Anlageperiode gültigen Konditionen weiterhin gelten. Der Kunde kann zum Zeitpunkt der Prolongation nicht wissen, zu welchem Zinssatz er prolongiert, da für die Prolongation derjenige Zinssatz herangezogen wird, der zum Zeitpunkt des Inkrafttretens der Prolongation aktuell gültig ist. Der Kunde ist an geeigneter Stelle (z.B. Kundenbedingungen) auf diesen Sachverhalt hinzuweisen.

Der Kunde kann einen Prolongationsauftrag ändern, indem er einen zweiten Prolongationsauftrag schickt und damit den bestehenden Auftrag überschreibt. Dies gilt jedoch nur, sofern der erste Auftrag noch nicht wirksam geworden ist.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Festgeldanlage prolongieren
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HKFGP
 Bezugssegment: -
 Segmentversion: 2
 Sender: Kunde
 Format: Festgeld

◆ Belegungsrichtlinien

Nr. 2: Anlagekonto

Es ist das Konto der zu prolongierenden Festgeldanlage einzustellen.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 92	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen

Nr. 3: Kontraktreferenz

Sofern eine Kontraktreferenz erteilt wurde, ist diese anzugeben.

Nr. 4-12:

Es sind die gültigen Daten der Festgeldanlage einzustellen. Diese dienen zu Plausibilitätsprüfungen.

Nr. 13: Zinsertrag voraussichtlich

Belegung nicht zulässig.

Nr. 14: Festgeldstatus

Belegung nicht zulässig.

Nr. 15: Prolongation

Es sind die Prolongationsdaten anzugeben.

◆ Beispiel

```
HKFGP:3:2+7654321:280:10020030+123+10000,:DEM+19
960701:19960831:3,25:A:10000,:DEM:19999,:DEM:4:6
0 Tage, 3,25%+1234567:280:10020030+J+1+1+1234567
:280:10020030+++++30:10000,:DEM:1'
```

b) Kreditinstitutsrückmeldung

◆ Format

Name: Festgeldprolongation bestätigen
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIFGP
 Bezugssegment: HKFGP
 Segmentversion: 2
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Anlagekonto	DEG	kto	#	M	1	
3	Kontraktreferenz	DE	id	#	K	1	
4	Anlagekonto alt	DEG	kto	#	K	1	
5	Kontraktreferenz alt	DE	id	#	K	1	

◆ Erläuterungen

s. „Festgeldänderung“

◆ Beispiel

```
HIFGP:3:2:3+7654322:280:10020030+124+7654321:280
:10020030+123'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen	Stand: 02.02.1998	Seite: 93

♦ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
0020	Festgeldanlage prolongiert
9210	Festgeldkonto existiert nicht
9210	Konto ist kein Festgeldkonto
9210	Laufzeit und Anlagebetrag entsprechen nicht den aktuellen Festgeldkonditionen
9210	Anlagebetrag geringer als Mindestaufstockungsbetrag

c) Bankparameterdaten

♦ Format

Name: Festgeldprolongation Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIFGPS
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

♦ Erläuterungen

Nr. 4: Parameter

Die DEG wird nicht belegt.

♦ Beispiel

HIFGPS:29:2:5+1+2'

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 94	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen

VII.3.5 Festgeldbestandsabfrage

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Festgeldbestand **anfordern**

Typ: Segment

Segmentart: Geschäftsvorfall

Kennung: HKFGB

Bezugssegment: -

Segmentversion: **2**

Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Anlagekonto	DEG	kto	#	M	1	
3	Kontraktreferenz	DE	id	#	K	1	
4	Alle Konten	DE	jn	#	M	1	
5	Maximale Anzahl Einträge	DE	num	..4	K	1	>0
6	Aufsetzpunkt	DE	an	..35	K	1	

◆ Erläuterungen

Nr. 2: Anlagekonto

Es ist die Kontoverbindung des gewünschten Festgeldkontos anzugeben.

Nr. 3: **Kontraktreferenz**

Sofern eine Kontraktreferenz erteilt wurde, kann diese hier angegeben werden.

Nr. 4: Alle Konten

Mit dieser Option kann gewählt werden, ob die Informationen nur zu dem angegebenen oder zu allen Anlagekonten des Kunden rückgemeldet werden sollen. Falls die Option „Alle Konten“ gewählt wird, ist in das DE „Anlagekonto“ ein beliebiges Anlagekonto des Kunden einzustellen. Falls noch keine Anlagekontonummer bekannt ist (s.o.) muß ersatzweise ein Kontokorrentkonto des Kunden eingestellt werden.

Nr. 5: Maximale Anzahl Einträge

Es kann die Anzahl der rückzumeldenden Festgeldkonten begrenzt werden (s. Kap. II.7.3).

Nr. 6: Aufsetzpunkt

Belegung nur zulässig, wenn vom Kreditinstitut ein Aufsetzpunkt rückgemeldet wurde (s. Kap. II.7.3).

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen	Stand: 02.02.1998	Seite: 95

◆ Beispiel

HKFGB:3:2+7654321:280:10020030+123+N'

b) Kreditinstitutsrückmeldung

◆ Beschreibung

Es sind jeweils die für die gegenwärtige Anlageperiode gültigen Daten der Festgeldanlage einzustellen.

Falls der Kunde „Alle Konten“ gewählt hat, ist das Segment für **jede Festgeldanlage** jeweils einmal einzustellen. **Falls der Kunde ein Anlagekonto angibt, so ist das Segment für jeden unter diesem Konto angelegten Kontrakt einzustellen, es sei denn, im Kundenauftrag wurde eine spezielle Kontraktreferenz angegeben.**

◆ Format

Name: Festgeldbestand rückmelden
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIFGB
 Bezugssegment: HKFGB
 Segmentversion: 2
 Sender: Kreditinstitut
 Format: Festgeld

◆ Belegungsrichtlinien

Nr. 2: Anlagekonto

Belegung ist verpflichtend.

Nr. 3: Kontraktreferenz

Sofern das Kreditinstitut für die Festgeldanlage eine Kontraktreferenz erteilt, wird diese hier zurückgemeldet.

Nr. 4: Anlagebetrag

Betrag, der für die aktuelle Anlageperiode gültig ist

Nr. 5: Festgeldkondition

Es ist die Kondition anzugeben, die für die aktuelle Anlageperiode gültig ist. Falls Sonderkonditionen vereinbart wurden, läßt sich u.U. kein Betragsintervall angeben. In diesem Fall ist die Belegung der Felder „Anlagebetrag von“ und „Anlagebetrag bis“ nicht erforderlich.

Nr. 12: Version der Konditionen

Belegung nicht zulässig

Nr. 13: Zinsertrag voraussichtlich

Das DE kann bei Bedarf belegt werden.

Nr. 14: Festgeldstatus

Das DE muß belegt werden.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 96	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen

Nr. 15:Prolongation

Nur zu belegen, wenn für den nächsten Anlagezeitraum eine Prolongation beantragt wurde.

◆ Beispiel

```
HIFGB:3:2:3+7654321:280:10020030+123+10000,:DEM+
19960701:19960831:3,25:A:10000,:DEM:19999,:DEM:4
:60 Tage, 3,25%+1234567:280:10020030+J+1+1+12345
67:280:10020030+++345,67:DEM+1+30:10000,:DEM:1'
```

◆ Ausgewählte Beispiele für Rückmeldungscoodes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
3010	Es liegen keine Festgeldanlagen vor
9210	Angegebenes Konto ist kein Festgeldkonto

c) Bankparameterdaten

◆ Format

Name: Festgeldbestand Parameter
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HIFGBS
Bezugssegment: HKVVB
Segmentversion: 1
Sender: Kreditinstitut
Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Die DEG wird nicht belegt.

◆ Beispiel

```
HIFGBS:30:2:5+1+2'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen	Stand: 02.02.1998	Seite: 97

VII.3.6 Widerruf einer Festgeldneuanlage

Dieser Geschäftsvorfall darf nur bei vorgemerkten Festgeldanlagen, d.h. terminierten Anlagen, die noch nicht wirksam geworden sind, gesendet werden. Bei aktiven Festgeldanlagen wird dieser Auftrag abgelehnt.

Dieser Auftrag ist nur möglich, wenn dem Kunden bei der Neuanlage eine Anlagekontonummer mitgeteilt wurde, mit der die zu widerrufende Festgeldanlage identifiziert werden kann.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Festgeldneuanlage widerrufen
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKFGW
Bezugssegment: -
Segmentversion: 2
Sender: Kunde
Format: Festgeld

◆ Belegungsrichtlinien

Nr. 2: Anlagekonto

Es ist das Konto der zu widerrufenden Festgeldanlage einzustellen.

Nr. 3: Kontraktreferenz

Sofern eine Kontraktreferenz erteilt wurde, ist diese anzugeben.

Nr. 4-12:

Es sind die gültigen Daten der Festgeldanlage einzustellen. Diese dienen zu Plausibilitätsprüfungen.

Nr. 13: Zinsertrag voraussichtlich

Belegung nicht zulässig.

Nr. 14: Festgeldstatus

Belegung nicht zulässig.

Nr. 15: Prolongation

Belegung nicht zulässig.

◆ Beispiel

```
HKFGW:3:2+7654321:280:10020030+123+10000,:DEM+19
960701:19960831:3,25:A:10000,:DEM:19999,:DEM:4:6
0 Tage, 3,25%+1234567:280:10020030+J+1+1+1234567
:280:10020030++38516:19960701:152245'
```

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 98	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen

b) Kreditinstitutsrückmeldung

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel
0010	Auftrag entgegengenommen
0020	Festgeldanlage storniert
9210	Widerruf nicht mehr möglich, da Festgeldanlage schon erfolgt ist

c) Bankparameterdaten

◆ Format

Name: Festgeldneuanlage widerrufen Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIFGWS
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Die DEG wird nicht belegt.

◆ Beispiel

HIFGWS:31:2:5+1+2'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen	Stand: 02.02.1998	Seite: 99

VII.3.7 Widerruf einer Festgeldprolongation

Mit Hilfe dieses Geschäftsvorfall kann ein noch nicht wirksam gewordener Auftrag für eine Festgeldprolongation storniert werden.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Festgeldprolongation widerrufen
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKFPW
Bezugssegment: -
Segmentversion: 2
Sender: Kunde
Format: Festgeld

◆ Belegungsrichtlinien

Nr. 2: Anlagekonto

Es ist das Konto der betreffenden Festgeldanlage einzustellen.

Nr. 3: Kontraktreferenz

Sofern eine Kontraktreferenz erteilt wurde, ist diese anzugeben.

Nr. 4-12:

Es sind die gültigen Daten der Festgeldanlage einzustellen. Diese dienen zu Plausibilitätsprüfungen.

Nr. 13: Zinsertrag voraussichtlich

Belegung nicht zulässig.

Nr. 14: Festgeldstatus

Belegung nicht zulässig.

Nr. 15: Prolongation

Es sind die Daten anzugeben, die der Kunde im Prolongationsauftrag angegeben hat.

◆ Beispiel

```
HKFPW:3:2+7654321:280:10020030+123+10000,:DEM+19
960701:19960831:3,25:A:10000,:DEM:19999,:DEM:4:6
0 Tage, 3,25%+1234567:280:10020030+J+1+1+1234567
:280:10020030+++++30:10000,:DEM:1'
```

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 100	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Termineinlagen

b) Kreditinstitutsrückmeldung

♦ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

♦ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel
0010	Auftrag entgegengenommen
0020	Festgeldprolongation storniert
9210	Für diese Festgeldanlage wurde keine Prolongation eingereicht
9210	Widerruf nicht mehr möglich, da Festgeldanlage schon prolongiert wurde

c) Bankparameterdaten

♦ Format

Name: Festgeldprolongation widerrufen Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIFPWS
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

♦ Erläuterungen

Nr. 4: Parameter

Die DEG wird nicht belegt.

♦ Beispiel

HIFPWS:32:2:5+1+2 '

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Wertpapiere	Stand: 02.02.1998	Seite: 101

VII.4 Wertpapiere

VII.4.1 Depotaufstellung

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Beschreibung

Die Depotaufstellung kann beliebige Papiere, auch in Fremdwährungen, umfassen.

◆ Format

Name: Depotaufstellung anfordern
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HKWPD
 Bezugssegment: -
 Segmentversion: 2
 Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Depot	DEG	kto	#	M	1	
3	Maximale Anzahl Einträge	DE	num	..4	K	1	>0
4	Aufsetzpunkt	DE	an	..35	K	1	

◆ Erläuterungen

Nr. 2: Depot

Es ist die jeweilige Depotnummer anzugeben.

Nr. 3: Maximale Anzahl Einträge

Es kann die Anzahl der rückzumeldenden Depotpositionen begrenzt werden (s. Kap. II.7.3).

Nr. 4: Aufsetzpunkt

Belegung nur zulässig, wenn vom Kreditinstitut ein Aufsetzpunkt rückgemeldet wurde (s. Kap. II.7.3).

◆ Beispiel

HKWPD:3:2+23456:280:10020030'

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 102	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Wertpapiere

b) Kreditinstitutsrückmeldung

◆ Format

Name: Depotaufstellung
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIWPD
 Bezugssegment: HKWPD
 Segmentversion: 2
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	MT 571	DE	bin	..	M	1	

◆ Erläuterungen

Nr. 2: Depotaufstellung

Es ist das SWIFT-Format MT 571 gemäß Spezifikation in den Anlagen (Kap. VIII.9.3.1) einzustellen. Auf die Verwendung des vom HBCI-Zeichensatz abweichenden SWIFT-Zeichensatzes¹ ist zu achten.



Da der MT 571 beliebig viele Wiederholungszyklen (Depositionen) enthalten kann, sollte vom Kundenprodukt die SWIFT-Blockbegrenzung bei der Entgegennahme des MT 571 nicht geprüft werden.

◆ Beispiel

HIWPD:3:2:3+@318@<MT 571>'

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
3010	Es liegen keine Einträge vor
9210	Keine gültige Kontonummer des Kunden
9210	Konto ist kein Depotkonto

¹ s. Kap. VIII.9.3

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Wertpapiere	Stand: 02.02.1998	Seite: 103

c) Bankparameterdaten

◆ Format

Name: Depotaufstellung Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIWPDS
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Depotaufstellung
 Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Eingabe Anzahl Einträge erlaubt	GD	jn	#	M	1	

Nr. 1: Eingabe Anzahl Einträge erlaubt

Es ist anzugeben, ob die Begrenzung der maximal rückzumeldenden Depotpositionen mit Hilfe des DE „Maximale Anzahl Einträge“ im Kundenauftrag kreditinstitutsseitig zulässig ist.

◆ Beispiel

HIWPDS:31:2:5+1+2+J'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Ausland	Stand: 02.02.1998	Seite: 105

VII.5 Zahlungsverkehr Ausland

VII.5.1 Zahlungsauftrag im Außenwirtschaftsverkehr

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Beschreibung

Der Datenaustausch im Auslandszahlungsverkehr ist durch das DTAZV-Format¹ standardisiert. Das DTAZV-Format ist transparent in ein Datenelement einzustellen.

Es kommen verschiedene Versionen des DTAZV zur Anwendung, die anhand der HBCI-Segmentversion unterschieden werden:

Altformat (Segmentversion 2):

Feld	Belegung
T 4a	Muß/Kann-Feld
T12	Es darf nur die Kontonummer des Begünstigten eingestellt werden.
T13	Angabe von 'EUR' nicht zugelassen
T18	Weisungsschlüssel '95' (Auftragswährung der Meldebeträge) ist nicht zugelassen
T19	Weisungsschlüssel '91' (Euro-Gegenwertzahlung) ist nicht zugelassen
T24	Kann-Feld; Stellvertretungsanzeige nicht zugelassen
U3	Muß-Feld
U4	Muß-Feld
U5	Angabe nur in DM möglich
V4	Angabe der Warenverzeichnis-Nummer (9 Stellen in Feld 4a und 4b)
V7	Angabe nur in DM möglich
V13	Angabe der Warenverzeichnis-Nummer (9 Stellen in Feld 4a und 4b)
V17	Angabe nur in DM möglich
W9	Angabe nur in DM möglich

Neuformat (Segmentversion 3):

Feld	Belegung
T 4a	Muß-Feld
T12	Es darf entweder die Kontonummer des Begünstigten oder alternativ der IBAN des Begünstigten eingestellt werden.
T13	zusätzlich Angabe von 'EUR' möglich
T18	Muß/Kann-Feld; Weisungsschlüssel '95' (Auftragswährung der Meldebeträge) ist zugelassen
T19	Muß/Kann-Feld; Weisungsschlüssel '91' (Euro-Gegenwertzahlung) ist zugelassen
T24	Muß/Kann-Feld; Stellvertretungsanzeige zugelassen

¹ s. Kap. VIII.9.2

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 106	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Ausland

Feld	Belegung
U3	Kann-Feld
U4	Kann-Feld
U5	Angabe in Auftragswährung
V4a	Angabe der Kapitel-Nr. des Warenverzeichnisses
V7	Angabe in Auftragswährung
V13a	Angabe der Kapitel-Nr. des Warenverzeichnisses
V17	Angabe in Auftragswährung
W9	Angabe in Auftragswährung

Das Neuformat kann ab 01.07.1998 genutzt werden, die Verwendung ist ab dem Start der Stufe 3 der EWWU obligatorisch. Das Altformat kann bis einschließlich 31.12.1998 verwendet werden und wird am 01.01.1999 ungültig.

Das Kreditinstitut gibt in den Bankparameterdaten an, welches bzw. welche dieser Formate (Segmentversionen) entgegengenommen werden können.

Bei Aufträgen, die den jeweiligen Meldepflichtgrenzbetrag überschreiten, ist die Meldepflicht an die Deutsche Bundesbank (Meldesätze U, V und W) zu beachten. Bei Aufträgen, die nicht der Meldepflicht unterliegen, können diese Datensätze entfallen.

Der Umfang der Plausibilitätsprüfung bei Auftragsannahme ist kreditinstitutsspezifisch. Die Prüfung auf vollständige Datenübertragung erfolgt anhand des Z-Satzes.



Die Präsentation der Eingabemaske ist Aufgabe des Herstellers des Kundenprodukts. So kann die Eingabe für den Kunden im Regelfall auf die unabdingbar notwendigen Eingabefelder begrenzt werden. Beispielsweise wäre daher auch die Anzeige des Euroüberweisungsformulars als Eingabemaske möglich. Es ist auf jeden Fall darauf zu achten, daß die Eingaben des Kunden vom Kundenprodukt in das gültige DTAZV-Format konvertiert werden.

Je nach Geschäftsvorfall sind unterschiedliche Kann- und Muß-Felder anzugeben. Im T-Satz sind im aktuellen DTAZV-Format folgende Felder Muß-Felder:

<u>Feldnr.:</u>	<u>Beschreibung:</u>
1	Satzlänge
2	Satzart
3	BLZ (Auftraggeber)
4a	ISO-Währungscode
4b	Kontonummer (Auftraggeber)
10a	Länderkennziffer (Empfänger)
10b	Name (Empfänger/Begünstigter)
13	Auftragswährung (Auftraggeber)
14a	Betrag (Vorkommastellen)
14b	Betrag (Nachkommastellen)
21	Kostenverrechnungsschlüssel
22	Kennzeichnung der Zahlungsart

Ebenfalls werden im Rahmen dieser Schnittstelle keine Vorgaben über die Erzeugung der Meldesätze an die Deutsche Bundesbank gemacht. Dem Kundenprodukt stehen hier folgende Möglichkeiten

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Ausland	Stand: 02.02.1998	Seite: 107

offen:

- ♦ automatische Erzeugung der Meldesätze
- ♦ Hinweis auf Meldepflicht an den Kunden
- ♦ Beschränkung auf nicht-meldepflichtige Auslandsüberweisungen

♦ Format

Name: Auslandsüberweisung
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HKAUB
 Bezugssegment: -
 Segmentversion: 2, 3
 Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	DTAZV-Datensatz	DE	bin	..	M	1	

♦ Erläuterungen

Nr. 2: DTAZV-Datensatz

Es ist der DTAZV-Datensatz gemäß Spezifikation in Kap. VIII.9.2 einzustellen.

♦ Beispiel

HKAUB : 3 : 3+@438@<DTAZV> '

b) Kreditinstitutsrückmeldung

♦ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

♦ Ausgewählte Beispiele für RückmeldungsCodes

Es gelten die RückmeldungsCodes der Einzelüberweisung. Zusätzlich gelten:

Code	Beispiel für Rückmeldungstext
9210	Ungültiges Format

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 108	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Zahlungsverkehr Ausland

c) Bankparameterdaten

◆ Format

Name: Auslandsüberweisung Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIAUBS
 Bezugssegment: HKVVB
 Segmentversion: 2, 3
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Auslandsüberweisung
 Typ: Datenelementgruppe

Nr.	Name	Typ	For- mat	Län- ge	Sta- tus	An- zahl	Restriktionen
1	Maximale Anzahl T-Sätze	GD	num	..4	M	1	

Nr. 1: Maximale Anzahl T-Sätze

Der Parameter gibt an, wie viele T-Sätze maximal in ein DTAZV-Format eingestellt werden dürfen. Für eine unbegrenzte Anzahl ist der Wert „0“ einzustellen.

◆ Beispiel

HIAUBS : 31 : 3 : 5+1+2+0 '

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Karten, Schecks und Formulare	Stand: 02.02.1998	Seite: 109

VII.6 Karten, Schecks und Formulare

VII.6.1 Bestellung

VII.6.1.1 Vordruckbestellung

Art und Umfang der vom Kunden zu bestellenden Vordrucke/Formulare variiert von Kreditinstitut zu Kreditinstitut. Angeboten werden können bspw. Überweisungs-, Lastschrift- oder Dauerauftragsformulare sowie insbesondere Formulare zu Geschäftsvorfällen, die zur Zeit noch nicht über HBCI unterstützt werden.

Die Bestellung von Zahlungsverkehrsvordrucken und Schecks ist identisch, da aus sicherheitstechnischer Sicht kein Unterschied besteht. Lediglich für die Bestellung von Reiseschecks ist ein separater Geschäftsvorfall vorgesehen.

Generell sollte für Kunden, die am Homebanking-Verfahren teilnehmen, jedoch das Einreichen von Aufträgen per Vordruck nicht mehr erforderlich sein. Daher soll die Formularbestellung durch den Kunden per Homebanking nur im Einzelfall erfolgen.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Beschreibung

Die Zusendung der Schecks und Vordrucke erfolgt standardmäßig an die Adresse, die kreditinstitutsseitig als Anschrift zum angegebenen Konto gespeichert ist.

Die Prüfung, wie viele Schecks des Kunden jeweils im Umlauf sind, und ggf. eine Sperrung weiterer Scheckbestellungen obliegt dem jeweiligen Kreditinstitut.

◆ Format

Name: Vordruckbestellung
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKVDB
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kontoverbindung Auftraggeber	DEG	kto	#	M	1	
3	Auslieferung	DE	num	1	M	1	
4	Formularcode	DE	num	..2	M	1	
5	Gewünschte Anzahl	DE	num	..3	K	1	>0
6	Adressaufdruck	DE	jn	#	K	1	
7	Adresse	DEG	adr	#	K	1	

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 110	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Karten, Schecks und Formulare

♦ Erläuterungen

Nr. 3: Auslieferung

Der Kunde hat anzugeben, ob die Vordrucke für ihn in der zuständigen Geschäftsstelle hinterlegt oder per Post zugesendet werden sollen.

Code	Bedeutung
1	Bereitlegung in der Geschäftsstelle
2	Zusendung per Post

Nr. 4: Formularcode

Die je Kreditinstitut angebotenen Formulare bzw. Schecks sind in den BPD eingestellt. Es dürfen nur die in den BPD angegebenen Formularcodes bestellt werden.

Nr. 5: Gewünschte Anzahl

In diesem DE kann der Kunde die gewünschte Anzahl der Formulare angeben. Diesem Wunsch muß jedoch vom Kreditinstitut nicht entsprochen werden, da die Anzahl abhängig von den institutsindividuellen Packungseinheiten ist. Gibt der Kunde keinen Wert an, so wird ihm die (kreditinstitutspezifische) Standardanzahl zugestellt.

Der Wert „0“ ist ungültig.

Nr. 6: Adressaufdruck

Für welche Formularcodes der Adressaufdruck möglich ist, ist in den BPD angegeben. Der Kunde hat in diesem Fall anzugeben, ob er einen Adressaufdruck auf seinen Formularen wünscht. Die für den Adressaufdruck notwendigen Daten werden den kreditinstitutsseitigen Verarbeitungssystemen entnommen. Eine Änderung dieser Daten durch den Kunden ist nicht möglich.

Nr. 7: Adresse

Die Belegung ist nur zulässig, wenn als Auslieferungsart „Zusendung per Post“ gewählt wurde. In diesem Fall kann hier bei Bedarf eine von der Standardadresse abweichende Zieladresse des Kunden angegeben werden.

Format: s. Kap. II.5.3.5

♦ Beispiel

```
HKVDB:3:1+1234567:280:10020030+2+10+20+N+Ernst M
üller::Bahnhofstr. 17:12345 Berlin'
```

b) Kreditinstitutsrückmeldung

♦ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Karten, Schecks und Formulare	Stand: 02.02.1998	Seite: 111

♦ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
9010	Kunde besitzt keine Scheckkarte
9010	Die Scheckkarte ist gesperrt
9010	Die maximale Anzahl ausgegebener Formulare wurde überschritten
9210	Keine gültige Kontonummer des Kunden
9210	Formular wird nicht angeboten
9210	Adressaufdruck nicht möglich

c) Bankparameterdaten

♦ Beschreibung

Hier legt das Kreditinstitut diejenigen Formulare fest, die vom Kunden bestellt werden können.

♦ Format

Name: Vordruckbestellung Parameter
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HIVDBS
Bezugssegment: HKVVB
Segmentversion: 1
Sender: Kreditinstitut
Format: Geschäftsvorfallparameter

♦ Erläuterungen

Nr. 4: Parameter

Name: Parameter Vordruckbestellung
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Formular	GDG			M	1..99	

Nr. 1: Formular

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Formularcode	GD	num	..2	M	1	
2	Formularbezeichnung	GD	an	..35	M	1	
3	Adressaufdruck möglich	GD	jn	#	M	1	

♦ Beispiel

HIVDBS:34:1:5+1+2+10:ec-Scheck:N:11:Barscheck:J:
12:Verrechnungsscheck:J:13:Überweisungsformular:
J'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Informationen	Stand: 02.02.1998	Seite: 113

VII.7 Informationen

VII.7.1 Freitextmeldungen

VII.7.1.1 Kundenmeldung

Dem Kunden wird die Möglichkeit gegeben, eine unstrukturierte, unformatierte Meldung (Freitext) an das Kreditinstitut zu senden. Gegenstand der Freitextmeldung können alle Aufträge sein, zu denen (noch) keine expliziten Geschäftsvorfälle existieren. Ferner können per Kundenmeldung beliebige Informationen ohne Auftragscharakter an das Kreditinstitut übermittelt werden.

Da der Kunde auch Aufträge in der Meldung übermitteln kann, ist die allgemeine Kundenmeldung stets zu signieren.

Die Behandlung der Meldung sowie die Reaktion auf die Meldung sind kreditinstitutsspezifisch und den entsprechenden Bedingungen des Kunde-Bank-Verhältnisses zu entnehmen. Insbesondere sollten mit Hilfe der Freitextmeldung keine zeitkritischen Aufträge gesendet werden.



Die Kundenmeldung soll nicht die Funktionalität eines Email-Dienstes (Adressierung, Anhängen von Anlagen, Formatierungsmöglichkeiten etc.) bieten, sondern diesen ergänzen. Es ist dem Kundenprodukt freigestellt, über die Kundenmeldung hinaus zusätzlich die Mailkomponente des jeweiligen Online-Dienstes anzubieten.

Kundenmeldungen sollten im Kundenprodukt gespeichert werden, um dem Kunden auch zu einem späteren Zeitpunkt einen Zugriff auf seine Meldungen zu ermöglichen.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Beschreibung

Der Kunde erhält lediglich eine Bestätigung des Eingangs seiner Meldung, jedoch keine Rückmeldung bzgl. der Bearbeitung oder Ausführung (sofern es sich um einen Auftrag handelt). Ebenso sind keine weiteren Informationen über den Verarbeitungsvorgang im Statusprotokoll abrufbar.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 114	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Informationen

◆ Format

Name: Kundenmeldung
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HKKDM
 Bezugssegment: -
 Segmentversion: 2
 Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kontoverbindung Auftraggeber	DEG	kto	#	M	1	
3	Kontowährung	DE	cur	#	K	1	
4	Freitextmeldung	DE	txt	.. 2048	M	1	
5	Betreff	DE	an	..35	K	1	

◆ Erläuterungen

Nr. 3: Kontowährung

Falls unter einer Kontonummer verschiedene Währungskonten geführt werden, kann hier durch Angabe des ISO-Währungscode eine entsprechende Einschränkung erfolgen, um das entsprechende Konto zu identifizieren.

Nr. 4: Freitextmeldung

Die maximale Länge der Freitextmeldung ist den BPD zu entnehmen. Meldungen, deren Länge diesen Wert übersteigen, werden abgelehnt. Die Daten dürfen nicht um führende oder nachfolgende Leerzeichen gekürzt werden.

Nr. 5: Betreff

Es kann das Thema der Meldung (Betreffzeile) eingestellt werden.

◆ Beispiel

```

HKKDM:4:2+1234567:280:10020030++Bitte schicken Sie mir Ihre Allgemeinen Geschäftsbedingungen. Danke Ernst Müller'
  
```

b) Kreditinstitutsrückmeldung

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Informationen	Stand: 02.02.1998	Seite: 115

♦ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0010	Meldung entgegengenommen
9140	Freitextmeldung zu lang
9210	Keine gültige Kontonummer des Kunden

c) Bankparameterdaten

♦ Format

Name: Kundenmeldung Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIKDMS
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

♦ Erläuterungen

Nr. 4: Parameter

Name: Parameter Kunden-/Gastmeldung
 Type: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Maximale Länge	GD	num	..4	M	1	>0

Nr. 1: Maximale Länge

Es ist die maximale Länge der Freitextmeldung in Byte (=Zeichen) anzugeben. Freitextmeldungen, die diese Länge überschreiten, werden abgewiesen.

♦ Beispiel

HIKDMS:47:2:5+1+2+1024'

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 116	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Informationen

VII.7.1.2 Gastmeldung

Um auch Nichtkunden die Möglichkeit zu geben, mit einem bestimmten Kreditinstitut zu kommunizieren (z.B. zur Anforderung von Informationen über das Leistungsspektrum, Angebote oder Preise), steht dieser Geschäftsvorfall zur Verfügung. Für das Format und die Beantwortung des Auftrages gilt dasselbe wie für den Geschäftsvorfall „Kundenmeldung“ (s.o.).

Die Angabe der/einer Kontoverbindung ist optional. Eine Signatur des Auftrages ist nicht erforderlich.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Gastmeldung
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKGAM
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kontoverbindung Auftraggeber	DEG	kto	#	K	1	
3	Freitextmeldung	DE	txt	.. 2048	M	1	
4	Betreff	DE	an	..35	K	1	

◆ Erläuterungen

Nr. 3: Freitextmeldung

Die maximale Länge der Freitextmeldung ist der BPD zu entnehmen. Meldungen, deren Länge diesen Wert übersteigen, werden abgelehnt. Die Daten dürfen nicht um führende oder nachfolgende Leerzeichen gekürzt werden.

Nr. 4: Betreff

Es kann das Thema der Meldung eingestellt werden.

◆ Beispiel

```
HKGAM:4:1++Bitte schicken Sie mir Informationen
zu Ihrem Leistungsspektrum. Danke Ernst Müller'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Informationen	Stand: 02.02.1998	Seite: 117

b) Kreditinstitutsrückmeldung

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

◆ Geschäftsvorfallspezifische RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
9140	Freitextmeldung länger als Vorgabe in der BPD

c) Bankparameterdaten

◆ Format

Name: Gastmeldung Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIGAMS
 Bezugssegment: HKVVB
 Segmentversion: 1
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Name: Parameter Kunden-/Gastmeldung
 Typ: Datenelementgruppe
 Format: s. „Allgemeine Kundenmeldung“

◆ Beispiel

HIGAMS : 48 : 1 : 5+1+2+512 '

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 118	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Informationen

VII.7.2 Formatierte Meldungen

VII.7.2.1 Kreditinstitutsangebote abholen

a) Kundenauftrag

◆ Beschreibung

Um Informationen zu bestimmten Themen anzufordern zu können, muß der Kunde zunächst ein Verzeichnis der lieferbaren Informationen von seinem Kreditinstitut abrufen. Diese Informationen können sowohl als Schriftdokumente als auch in Dateiform vorliegen.



Um zu vermeiden, daß für das Abholen der Angebote und das darauffolgende Bestellen der Informationen nicht jeweils die physikalische Verbindung erneut aufgebaut werden muß, sollten diese beiden Aufträge im Online-Modus erfolgen.

Realisierung Bank: optional

Realisierung Kunde: optional

◆ Format

Name: Kreditinstitutsangebote anfordern
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKKIA
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Maximale Anzahl Einträge	DE	num	..4	K	1	>0
3	Aufsetzpunkt	DE	an	..35	K	1	

◆ Erläuterungen

Nr. 2: Maximale Anzahl Einträge

Es kann die Anzahl der rückzumeldenden Kreditinstitutsangebote begrenzt werden (s. Kap. II.7.3).

Nr. 3: Aufsetzpunkt

Belegung nur zulässig, wenn vom Kreditinstitut ein Aufsetzpunkt rückgemeldet wurde (s. Kap. II.7.3).

◆ Beispiel

HKKIA:4:1'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Informationen	Stand: 02.02.1998	Seite: 119

b) Kreditinstitutsrückmeldung

◆ Format

Name: Kreditinstitutsangebote rückmelden
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIKIA
 Bezugssegment: HKKIA
 Segmentversion: 1
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Informationen	DEG			K	0..n	

◆ Erläuterungen

Nr. 2: DEG „Informationen“

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Informationscode	GD	an	..10	M	1	
2	Beschreibung	GD	an	..35	M	1	
3	Informationsart	GD	an	1	M	1	T, S
4	Version der Information	GD	dat	#	K	1	
5	Format der Information	GD	an	..3	K	1	
6	Erläuterungen	GD	an	..35	K	5	

Nr. 1: Informationscode

Hier ist ein Code einzustellen, der die Information eindeutig kennzeichnet.



Um im Kundenprodukt eine Sortierung nach Themengebieten etc. zu ermöglichen, kann das Kreditinstitut die Angebote anhand des Codes strukturieren. Die Klassifizierung kann von jedem Kreditinstitut selbst gebildet werden.

Bsp.: 3500: Lebensversicherungen
 3510: Allgemeines
 3511: Informationen zu Lebensversicherungen
 3512: Konditionen für Lebensversicherungen

Nr. 3: Informationsart

Die Informationsart gibt an, in welcher Form die Information vorliegt. Falls der Informationscode eine Themenüberschrift angibt, wird das DE mit „T“ belegt.

Code	Beispiel für Rückmeldungstext
D	Datei (z.Zt. noch nicht zulässig)
S	Schriftdokument
T	Themenüberschrift

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 120	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Informationen

Nr. 4: Version der Information

Datum der letzten Änderung.

Nr. 5: Format der Information

Die Einstellung eines Formats gilt nur für die Informationsart „D“ und wird im derzeitigen Stadium ignoriert. Zu einem späteren Zeitpunkt könnten hier Informationen über das Format der Datei („GIF“, „JPG“, „RTF“ etc.) eingestellt werden.

Nr. 6: Erläuterungen

Freitext, der die Art der Information näher erläutert.

◆ Beispiel

```
HIKIA:5:1:5+3500:Lebensversicherungen:T+3510:Allgemeines:T+3511:Infos zur Lebensversicherung:S+3512:Tarife für Lebensversicherungen:S'
```

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
3010	Z.Zt. sind keine Angebote abrufbar
9210	Keine gültige Kontonummer des Kunden

c) Bankparameterdaten

◆ Format

Name: Kreditinstitutsangebote Parameter
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HIKIAS
Bezugssegment: HKVVB
Segmentversion: 1
Sender: Kreditinstitut
Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Die DEG wird nicht belegt.

◆ Beispiel

```
HIKIAS:49:1:5+1+2'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Informationen	Stand: 02.02.1998	Seite: 121

VII.7.2.2 Informationsbestellung

Dem Kunden wird die Möglichkeit geboten, schriftliche Informationen zu bestimmten Themen strukturiert anzufordern. Zum Abholen von in Dateiform vorliegender Informationen dient dagegen zukünftig der Geschäftsvorfall „Datei abholen“.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Beschreibung

Um eine Übersicht der aktuell lieferbaren Informationen zu erhalten, hat der Kunde zunächst den Auftrag „Kreditinstitutsangebote abholen“ auszuführen. Die Informationen werden dem Kunden in der Regel auf dem Postweg zugeschickt. Empfängeradresse ist die im Kreditinstitut gespeicherte Kundenadresse. Optional kann eine hiervon abweichende Empfängeradresse angegeben werden. Bei Nichtkunden muß eine Empfängeradresse angegeben werden.

Eine Online-Rückmeldung des Kreditinstituts erfolgt nicht. Der Kunde erhält lediglich eine Bestätigung des Eingangs seiner Meldung. Ebenso sind keine Informationen über den Verarbeitungsvorgang im Statusprotokoll abrufbar.

Der Kunde hat kein Anrecht auf Zustellung der gewünschten Informationen, da diese evtl. momentan nicht vorrätig sind.

◆ Format

Name: Informationen anfordern
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKINF
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Informationscodes	DEG			M	1	
3	Adresse	DEG	adr	#	K	1	

◆ Erläuterungen

Nr. 2: Informationscodes

Es sind gültige Codes aus dem Angebotsverzeichnis des Kreditinstituts anzugeben.

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Informationscode	GD	an	..10	M	1..9	

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 122	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Informationen

Nr. 3: Adresse

s. Kap. II.5.3.5

♦ Beispiel

```
HKINF:3:1+3511:3512:3513+Ernst Müller::Bahnhofstr. 17:12345 Berlin'
```

b) Kreditinstitutsrückmeldung

♦ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

♦ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
9210	Keine gültige Kontonummer des Kunden
9210	Informationscode wird nicht angeboten

c) Bankparameterdaten

♦ Format

Name: Informationsanforderung Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIINFS
 Bezugssegment: HKVVB
 Segmentversion: 1
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

♦ Erläuterungen

Nr. 4: Parameter

Die DEG wird nicht belegt.

♦ Beispiel

```
HIINFS:50:1:5+1+2'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Informationen	Stand: 02.02.1998	Seite: 123

VII.7.2.3 Terminvereinbarung

Dem Kunden wird die Möglichkeit geboten, einen strukturierten Terminwunsch für ein Beratungsgespräch an das Kreditinstitut zu senden. Eine Online-Rückmeldung des Kreditinstituts, d.h. eine Terminbestätigung, erfolgt nicht. Der Kunde erhält lediglich eine Bestätigung des Eingangs seiner Meldung. Ebenso sind keine Informationen über den Verarbeitungsvorgang im Statusprotokoll abrufbar.

Die Angaben sind weder für den Kunden noch für das Kreditinstitut verbindlich. Der Termin gilt erst nach schriftlicher oder telefonischer Bestätigung durch das Kreditinstitut als vereinbart.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Format

Name: Terminvereinbarung
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HKTMV
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Datum	DE	dat	#	K	1	
3	Uhrzeit	DE	tim	#	K	1	
4	Geschäftsstelle	DE	an	..35	K	1	
5	Kundenberater	DE	an	..35	K	1	
6	Telefonnummer für Bestätigung	DE	an	..35	K	1	
7	Informationscode	DE	an	..10	K	1	
8	Thema	DE	an	..200	K	1	

◆ Erläuterungen

Nr. 2: Datum

Einzustellen ist das gewünschte Datum des Termins. Wird kein Datum angegeben, so wird diese Nachricht vom Kreditinstitut als Beratungswunsch ohne konkreten Terminvorschlag aufgefaßt. Das Kreditinstitut sollte sich daraufhin mit dem Kunden in Verbindung setzen, um einen Termin zu vereinbaren.

Nr. 3: Uhrzeit

Einzustellen ist die gewünschte Uhrzeit des Termins. Für den Fall, das keine Uhrzeit angegeben ist, gelten dieselben Modalitäten wie für ein fehlendes Datum.

Kapitel: VII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 124	Stand: 02.02.1998	Kapitel: Geschäftsvorfälle Abschnitt: Informationen

Nr. 4: Geschäftsstelle

Hier kann der Kunde die Geschäftsstelle angeben, in der er das Gespräch führen möchte. Wird kein Wert eingestellt, so wird die dem Kunden über seine Kontonummer zugeordnete Geschäftsstelle angenommen.

Nr. 5: Kundenberater

Falls der Kunde mit einem bestimmten Berater Kontakt aufnehmen möchte, kann er hier einen entsprechenden Wunsch äußern.

Nr. 6: Telefonnummer für Bestätigung

Um eine telefonische Bestätigung zu ermöglichen, kann der Kunde hier eine Telefonnummer angeben, unter der er zu den gewöhnlichen Banköffnungszeiten zu erreichen ist.

Nr. 7: Informationscode

Hier kann der Kunde einen Informationscode (s. Kap. VII.7.2.1) einstellen, um das Gesprächsthema vorab mitzuteilen.

Nr. 8: Thema

Hier kann der Kunde zusätzlich oder alternativ zum Informationscode das Thema des Gesprächs im Klartext nennen, um dem Kundenberater eine Vorbereitung auf das Gespräch zu ermöglichen.

◆ Beispiel

```
HKTMV:4:1+19960701+160000++Herr Schulze+0228-1234567++Wertpapierberatung'
```

b) Kreditinstitutsrückmeldung

◆ Erläuterungen

Es werden keine Datensegmente zurückgemeldet.

◆ Ausgewählte Beispiele für Rückmeldungscodes

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
9210	Datum liegt zu weit in der Zukunft
9210	Datum liegt nicht in der Zukunft
9210	Keine gültige Kontonummer des Kunden

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VII
Kapitel: Geschäftsvorfälle Abschnitt: Informationen	Stand: 02.02.1998	Seite: 125

c) Bankparameterdaten

◆ Format

Name: Terminvereinbarung Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HITMVS
 Bezugssegment: HKVVB
 Segmentversion: 1
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Die DEG wird nicht belegt.

◆ Beispiel

HITMVS:51:1:5+1+2 '

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Inhaltsverzeichnis	Stand: 02.02.1998	Seite: 1

VIII. ANLAGEN

VIII.1 Übersicht der Segmentkennungen	5
VIII.2 Übersicht der HBCI-Elemente.....	9
VIII.2.1 Nachrichten.....	9
VIII.2.2 Segmentfolgen	10
VIII.2.3 Segmente	11
VIII.2.4 Datenelementgruppen	14
VIII.2.5 Datenelemente	16
VIII.2.6 HBCI-Elemente allgemein.....	20
VIII.3 Übersicht Nachrichtenaufbau	29
VIII.3.1 Standarddialog	30
VIII.3.2 Anonymer Dialog	31
VIII.3.3 Synchronisierung	32
VIII.3.4 Kommunikationszugang	33
VIII.3.5 Änderung eines öffentlichen Schlüssels des Kunden.....	34
VIII.3.6 Erstmalige Anforderung der öffentlichen Schlüssel des Kreditinstituts	35
VIII.3.7 Erstmalige Übermittlung der öffentlichen Schlüssel des Kunden.....	36
VIII.3.8 Schlüsselsperrung durch den Kunden	37
VIII.3.9 Verschlüsselter Dialog	38
VIII.4 HBCI-Basiszeichensätze	39
VIII.4.1 ISO 8859-1 Subset Deutsch	39
VIII.4.2 ISO 8859-1 Subset Englisch.....	39
VIII.4.3 ISO 8859-1 Subset Französisch	40
VIII.5 Beispieldialog	41
VIII.5.1 Nachricht „Dialoginitialisierung“.....	41
VIII.5.2 Nachricht „Einzelüberweisung“	44
VIII.5.3 Nachricht „Saldenabfrage“	46
VIII.5.4 Nachricht „Dialogbeendigung“	47
VIII.6 Transportmedienspezifische Festlegungen	49
VIII.6.1 T-Online	49
VIII.6.1.1 ETSI 300 072 („CEPT“)	49
VIII.6.1.2 EHKP	52
VIII.6.1.3 BtxFIF	52

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 2	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Inhaltsverzeichnis

VIII.6.2 TCP/IP	55
VIII.6.2.1 Internet (WWW)	55
VIII.6.2.2 Direktzugang	55
VIII.6.2.2.1 Protokollanforderungen	55
VIII.6.2.2.2 Sicherheitsanforderungen	56
VIII.6.3 Sonstige Kommunikationsdienste	56
VIII.7 Abruf von Kommunikationszugangsdaten	57
VIII.8 Chipapplikation für DDV	63
VIII.8.1 DF_Banking	64
VIII.8.2 EFs im DF_Banking	65
VIII.8.2.1 EF_KEY	65
VIII.8.2.2 EF_KEYD	66
VIII.8.2.3 EF_AUT	67
VIII.8.2.4 EF_AUTD	68
VIII.8.2.5 EF_PWD1	69
VIII.8.2.6 EF_PWDD1	70
VIII.8.2.7 EF_BNK	71
VIII.8.2.8 EF_MAC	73
VIII.8.2.9 EF_SEQ	74
VIII.8.3 Platzbedarf der Applikation im Chip	75
VIII.8.4 Chipkarten- bzw. Endgeräteabläufe	76
VIII.8.4.1 Startdialog	77
VIII.8.4.2 Nachricht generieren	78
VIII.8.4.3 Nachricht signieren	79
VIII.8.4.4 Nachricht verschlüsseln	80
VIII.8.4.5 Übertragungsdialog	81
VIII.8.5 Makros	83
VIII.8.5.1 MAC-Berechnung	83
VIII.8.5.2 MAC-Prüfung	84
VIII.8.5.3 Verschlüsselung	85
VIII.8.5.4 Entschlüsselung	86
VIII.8.6 Beispiel für einen HBCI-Dialog mit Chipkarte	87
VIII.9 Verwendete Finanzdatenformate	89
VIII.9.1 DTAUS	89
VIII.9.2 DTAZV	100
VIII.9.3 SWIFT-Formate	121
VIII.9.3.1 MT 571	122
VIII.9.3.2 MT 940	128
VIII.9.3.3 MT 942	137
VIII.10 Berechnung der Prüfziffer für interne Zuordnungsdaten (Kunden-Referenznummer)	140
VIII.10.1 Rechengang	140
VIII.10.2 Beispiel	141

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Inhaltsverzeichnis	Stand: 02.02.1998	Seite: 3

VIII.11 Länderkennzeichen und Währungscode..... 142

VIII.12 Verweise auf verwendete Dokumente 143

VIII.12.1 Allgemeines 143

VIII.12.2 Sicherheit..... 143

VIII.12.3 Transportmedienspezifische Festlegungen 144

VIII.12.4 Geschäftsvorfälle 144

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Inhaltsverzeichnis	Stand: 02.02.1998	Seite: 5

VIII.1 Übersicht der Segmentkennungen

Kennung	Segmentname	Art ¹	Sender ²	Version	zusätzlich ³	Kapitel
HIAUBS	Auslandsüberweisung Parameter	GV	I	3	2	VII.5.1
HIBPA	Bankparameter allgemein	AD	I	2		IV.2
HIDAA	Dauerauftragsänderungsvormerkungen rückmelden	GV	I	1		VII.1.1.4.5
HIDAAS	Dauerauftragsänderungsvormerkungen Parameter	GV	I	1		VII.1.1.4.5
HIDAB	Dauerauftragsbestand rückmelden	GV	I	1		VII.1.1.4.4
HIDABS	Dauerauftragsbestand Parameter	GV	I	1		VII.1.1.4.4
HIDAE	Dauerauftragseinrichtung bestätigen	GV	I	2		VII.1.1.4.1
HIDAES	Dauerauftrag einrichten Parameter	GV	I	2		VII.1.1.4.1
HIDALS	Dauerauftrag löschen Parameter	GV	I	1		VII.1.1.4.6
HIDAN	Dauerauftragsänderung bestätigen	GV	I	2		VII.1.1.4.2
HIDANS	Dauerauftrag ändern Parameter	GV	I	2		VII.1.1.4.2
HIDAS	Dauerauftragsaussetzung bestätigen	GV	I	1		VII.1.1.4.3
HIDASS	Dauerauftrag aussetzen Parameter	GV	I	1		VII.1.1.4.3
HIFGA	Festgeldänderung bestätigen	GV	I	2		VII.3.3
HIFGAS	Festgeld ändern Parameter	GV	I	2		VII.3.3
HIFGB	Festgeldbestand rückmelden	GV	I	2		VII.3.5
HIFGBS	Festgeldbestand Parameter	GV	I	2		VII.3.5
HIFGK	Festgeldkonditionen rückmelden	GV	I	1		VII.3.1
HIFGKS	Festgeldkonditionen Parameter	GV	I	1		VII.3.1
HIFGN	Festgeldneuanlage bestätigen	GV	I	2		VII.3.2
HIFGNS	Festgeldneuanlage Parameter	GV	I	2		VII.3.2
HIFGP	Festgeldprolongation bestätigen	GV	I	2		VII.3.4
HIFGPS	Festgeldprolongation Parameter	GV	I	2		VII.3.4
HIFGWS	Festgeldneuanlage widerrufen Parameter	GV	I	2		VII.3.6
HIFPWS	Festgeldprolongation widerrufen Parameter	GV	I	2		VII.3.7
HIGAMS	Gastmeldung Parameter	GV	I	1		VII.7.1.2
HIINFS	Informationsanforderung Parameter	GV	I	1		VII.7.2.2
HIISA	Übermittlung eines öffentlichen Schlüssels	AD	I	2		VI.6.1.3
HIKAN	Kontoumsätze rückmelden/neue Umsätze	GV	I	4	3	VII.2.1.2
HIKANS	Kontoumsätze/neu Parameter	GV	I	4	3	VII.2.1.2
HIKAZ	Kontoumsätze rückmelden/Zeitraum	GV	I	4	3	VII.2.1.1
HIKAZS	Kontoumsätze/Zeitraum Parameter	GV	I	4	3	VII.2.1.1
HIKDMS	Kundenmeldung Parameter	GV	I	2		VII.7.1.1
HIKIA	Kreditinstitutsangebote rückmelden	GV	I	1		VII.7.2.1
HIKIAS	Kreditinstitutsangebote Parameter	GV	I	1		VII.7.2.1
HIKIM	Kreditinstitutsmeldung	AD	I	2		III.3.2.5
HIKOM	Kommunikationszugang rückmelden	GV	I	2		VIII.7
HIKOMS	Kommunikationszugang Parameter	GV	I	2		VIII.7
HIKPV	Komprimierungsverfahren	AD	I	1		IV.5

¹ AD: Administration, GV: Geschäftsvorfall

² K: Kunde, I: Kreditinstitut

³ Segmentversionen, die in der aktuellen HBCI-Version darüber hinaus zugelassen werden können (In der vorliegenden HBCI-Version werden keine zusätzlichen Segmentversionen unterstützt, d.h. es sind nur die in der aktuellen HBCI-Version definierten Segmentversionen zulässig).

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 6	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Inhaltsverzeichnis

Kennung	Segmentname	Art ¹	Sen- der ²	Ver- sion	zusätz- lich ³	Kapitel
HILASS	Lastschrift Parameter	GV	I	2		VII.1.1.5
HIPRO	Statusprotokoll rückmelden	GV	I	2		III.7
HIPROS	Statusprotokoll Parameter	GV	I	2		III.7
HIRMG	Rückmeldungen zur Gesamtnachricht	AD	I	2		II.8.2
HIRMS	Rückmeldung zu Segmenten	AD	I	2		II.8.3
HISAL	Saldenrückmeldung	GV	I	3		VII.2.2
HISALS	Saldenabfrage Parameter	GV	I	3		VII.2.2
HISHV	Sicherheitsverfahren	AD	I	2		IV.4
HISLAS	Sammellastschrift Parameter	GV	I	3	2	VII.1.2.2
HISSP	Bestätigung der Schlüsselsperrung	AD	I	2		VI.6.1.5
HISUBS	Sammelüberweisung Parameter	GV	I	3	2	VII.1.2.1
HISYN	Synchronisierungsantwort	AD	I	3		III.8.2.2
HITMVS	Terminvereinbarung Parameter	GV	I	1		VII.7.2.3
HITUA	Änderung terminierter Überweisung be- stätigen	GV	I	2		VII.1.1.3.2
HITUAS	Terminierte Überweisung ändern Para- meter	GV	I	2		VII.1.1.3.2
HITUB	Bestand terminierter Überweisungen rück- melden	GV	I	1		VII.1.1.3.3
HITUBS	Bestand terminierter Überweisungen Pa- rameter	GV	I	1		VII.1.1.3.3
HITUE	Einreichung terminierter Überweisung be- stätigen	GV	I	2		VII.1.1.3.1
HITUES	Terminierte Überweisung einreichen Pa- rameter	GV	I	2		VII.1.1.3.1
HITULS	Terminierte Überweisung löschen Para- meter	GV	I	1		VII.1.1.3.4
HIUEBS	Einzelüberweisung Parameter	GV	I	2		VII.1.1.1
HIUPA	Userparameter allgemein	AD	I	2		V.2
HIUPD	Kontoinformation	AD	I	3		V.3
HIVDBS	Vordruckbestellung Parameter	GV	I	1		VII.6.1.1
HIWPD	Depotaufstellung	GV	I	2		VII.4.1
HIWPDS	Depotaufstellung Parameter	GV	I	2		VII.4.1
HKAUB	Auslandsüberweisung	GV	K	3	2	VII.5.1
HKDAA	Dauerauftragsänderungsvormerkungen anfordern	GV	K	1		VII.1.1.4.5
HKDAB	Dauerauftragsbestand anfordern	GV	K	1		VII.1.1.4.4
HKDAE	Dauerauftrag einrichten	GV	K	2		VII.1.1.4.1
HKDAL	Dauerauftrag löschen	GV	K	1		VII.1.1.4.6
HKDAN	Dauerauftrag ändern	GV	K	2		VII.1.1.4.2
HKDAS	Dauerauftrag aussetzen	GV	K	1		VII.1.1.4.3
HKEND	Dialogende	AD	K	1		III.4.1.2
HKFGA	Festgeldanlage ändern	GV	K	2		VII.3.3
HKFGB	Festgeldbestand anfordern	GV	K	2		VII.3.5
HKFGK	Festgeldkonditionen anfordern	GV	K	1		VII.3.1
HKFGN	Festgeldneuanlage	GV	K	2		VII.3.2
HKFGP	Festgeldanlage prolongieren	GV	K	2		VII.3.4
HKFGW	Festgeldneuanlage widerrufen	GV	K	2		VII.3.6
HKFPW	Festgeldprolongation widerrufen	GV	K	2		VII.3.7
HKGAM	Gastmeldung	GV	K	1		VII.7.1.2
HKIDN	Identifikation	AD	K	2		III.3.1.2
HKINF	Informationen anfordern	GV	K	1		VII.7.2.2
HKISA	Anforderung eines öffentlichen Schlüssels	AD	K	2		VI.6.1.2

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Inhaltsverzeichnis	Stand: 02.02.1998	Seite: 7

Kennung	Segmentname	Art ¹	Sender ²	Version	zusätzlich ³	Kapitel
HKKAN	Kontoumsätze anfordern/neue Umsätze	GV	K	4	3	VII.2.1.2
HKKAZ	Kontoumsätze anfordern/Zeitraum	GV	K	4	3	VII.2.1.1
HKKDM	Kundenmeldung	GV	K	2		VII.7.1.1
HKKIA	Kreditinstitutsangebote anfordern	GV	K	1		VII.7.2.1
HKKOM	Kommunikationszugang anfordern	GV	K	2		VIII.7
HKLAS	Einzellastschrift	GV	K	2		VII.1.1.5
HKPRO	Statusprotokoll anfordern	GV	K	2		III.7
HKSAK	Schlüsseländerung	AD	K	2		VI.6.1.1
HKSAL	Saldenabfrage	GV	K	3		VII.2.2
HKSLA	Sammellastschrift	GV	K	3	2	VII.1.2.2
HKSSP	Schlüsselsperrung	AD	K	2		VI.6.1.4
HKSUB	Sammelüberweisung	GV	K	3	2	VII.1.2.1
HKSYN	Synchronisierung	AD	K	2		III.8.1.2
HKTMV	Terminvereinbarung	GV	K	1		VII.7.2.3
HKTUA	Terminierte Überweisung ändern	GV	K	2		VII.1.1.3.2
HKTUB	Bestand terminierter Überweisungen anfordern	GV	K	1		VII.1.1.3.3
HKTUE	Terminierte Überweisung einreichen	GV	K	2		VII.1.1.3.1
HKTUL	Terminierte Überweisung löschen	GV	K	1		VII.1.1.3.4
HKUEB	Einzelüberweisung	GV	K	2		VII.1.1.1
HKVDB	Vordruckbestellung	GV	K	1		VII.6.1.1
HKVVB	Verarbeitungsvorbereitung	AD	K	2		III.3.1.3
HKWPD	Depotaufstellung anfordern	GV	K	2		VII.4.1
HNHBK	Nachrichtenkopf	AD	K/I	2		II.6.2
HNHBS	Nachrichtenabschluß	AD	K/I	1		II.6.3
HNSHA	Signaturabschluß	AD	K/I	1		VI.5.3
HNSHK	Signaturkopf	AD	K/I	3		VI.5.2
HNVSD	Verschlüsselte Daten	AD	K/I	1		VI.5.5
HNVSK	Verschlüsselungskopf	AD	K/I	2		VI.5.4

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente	Stand: 02.02.1998	Seite: 9

VIII.2 Übersicht der HBCI-Elemente

VIII.2.1 Nachrichten

Nr.	Name	Ken- nung	Sen- der ¹	Kapitel
1	Änderung eines öffentlichen Schlüssels des Kunden	N1	K	VI.6.2.1
2	Antwort auf Dialoginitialisierung	N2	I	III.3.2.1
3	Antwort auf anonyme Dialoginitialisierung	N3	I	III.5.1
4	Antwort auf Kommunikationszugang	N4	I	VIII.7
5	Bestätigung der Schlüsselsperrung durch das Kreditinstitut	N5	I	VI.6.2.4
6	Dialoginitialisierung	N6	K	III.3.1.1
7	Dialoginitialisierung bei anonymem Zugang	N7	K	III.5.1
8	Dialogbeendigung	N8	K	III.4.1.1
9	Dialogbeendigung bei anonymem Zugang	N9	K	III.5.3
10	Erstmalige Anforderung der Schlüssel des Kreditinstituts	N10	K	VI.6.2.2
11	Erstmalige Übermittlung der Schlüssel des Kreditinstituts	N11	I	VI.6.2.2
12	Erstmalige Übermittlung der Schlüssel des Kunden	N12	K	VI.6.2.3
13	Kommunikationszugang	N13	K	VIII.7
14	Kreditinstitutsnachricht allgemein	N14	I	II.8.1
15	Kundennachricht allgemein	N15	K	II.7.1
16	Kundennachricht allgemein bei anonymem Zugang	N16	K	III.5.2
17	Sperrung eines Schlüssels durch den Kunden	N17	K	VI.6.2.4
18	Synchronisierungsnachricht	N18	K	III.8.1.1
19	Synchronisierungsantwortnachricht	N19	I	III.8.2.1
20	Verschlüsselte Nachricht	N20	K/I	II.9

¹ K: Kunde, I: Kreditinstitut

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 10	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente

VIII.2.2 Segmentfolgen

Nr.	Name	Sender ²	Kapitel
1	Aufträge	K	II.7.2
2	Bankparameterdaten	I	IV.1
3	Datensegmente	I	II.8.4
4	Parameterdaten	I	IV.7
5	Userparameterdaten	I	V.1

² K: Kunde, I: Kreditinstitut

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente	Stand: 02.02.1998	Seite: 11

VIII.2.3 Segmente

Nr.	Name	Kennung	Art ³	Sender ⁴	Kapitel
1	Änderung terminierter Überweisung bestätigen	HITUA	GV	I	VII.1.1.3.2
2	Anforderung eines öffentlichen Schlüssels	HKISA	AD	K	VI.6.1.2
3	Auslandsüberweisung	HKAUB	GV	K	VII.5.1
4	Auslandsüberweisung Parameter	HIAUBS	GV	I	VII.5.1
5	Bankparameter allgemein	HIBPA	AD	I	IV.2
6	Bestand terminierter Überweisungen anfordern	HKTUB	GV	K	VII.1.1.3.3
7	Bestand terminierter Überweisungen Parameter	HITUBS	GV	I	VII.1.1.3.3
8	Bestand terminierter Überweisungen rück-melden	HITUB	GV	I	VII.1.1.3.3
9	Bestätigung der Schlüsselsperrung	HISSP	AD	I	VI.6.1.5
10	Dauerauftrag ändern	HKDAN	GV	K	VII.1.1.4.2
11	Dauerauftrag ändern Parameter	HIDANS	GV	I	VII.1.1.4.2
12	Dauerauftrag aussetzen	HKDAS	GV	K	VII.1.1.4.3
13	Dauerauftrag aussetzen Parameter	HIDASS	GV	I	VII.1.1.4.3
14	Dauerauftrag einrichten	HKDAE	GV	K	VII.1.1.4.1
15	Dauerauftrag einrichten Parameter	HIDAES	GV	I	VII.1.1.4.1
16	Dauerauftrag löschen	HKDAL	GV	K	VII.1.1.4.6
17	Dauerauftrag löschen Parameter	HIDALS	GV	I	VII.1.1.4.6
18	Dauerauftragsänderung bestätigen	HIDAN	GV	I	VII.1.1.4.2
19	Dauerauftragsänderungsvormerkungen anfor- dern	HKDAA	GV	K	VII.1.1.4.5
20	Dauerauftragsänderungsvormerkungen Para- meter	HIDAAS	GV	I	VII.1.1.4.5
21	Dauerauftragsänderungsvormerkungen rück- melden	HIDAA	GV	I	VII.1.1.4.5
22	Dauerauftragsaussetzung bestätigen	HIDAS	GV	I	VII.1.1.4.3
23	Dauerauftragsbestand anfordern	HKDAB	GV	K	VII.1.1.4.4
24	Dauerauftragsbestand Parameter	HIDABS	GV	I	VII.1.1.4.4
25	Dauerauftragsbestand rückmelden	HIDAB	GV	I	VII.1.1.4.4
26	Dauerauftragseinrichtung bestätigen	HIDAE	GV	I	VII.1.1.4.1
27	Depotaufstellung	HIWPD	GV	I	VII.4.1
28	Depotaufstellung anfordern	HKWPD	GV	K	VII.4.1
29	Depotaufstellung Parameter	HIWPDS	GV	I	VII.4.1
30	Dialogende	HKEND	AD	K	III.4.1.2
31	Einreichung terminierter Überweisung bestätigen	HITUE	GV	I	VII.1.1.3.1
32	Einzellastschrift	HKLAS	GV	K	VII.1.1.5
33	Einzelüberweisung	HKUEB	GV	K	VII.1.1.1
34	Einzelüberweisung Parameter	HIUEBS	GV	I	VII.1.1.1
35	Festgeld ändern Parameter	HIFGAS	GV	I	VII.3.3
36	Festgeldänderung bestätigen	HIFGA	GV	I	VII.3.3
37	Festgeldanlage ändern	HKFGA	GV	K	VII.3.3
38	Festgeldanlage prolongieren	HKFGP	GV	K	VII.3.4
39	Festgeldbestand anfordern	HKFGB	GV	K	VII.3.5
40	Festgeldbestand Parameter	HIFGBS	GV	I	VII.3.5
41	Festgeldbestand rückmelden	HIFGB	GV	I	VII.3.5
42	Festgeldkonditionen anfordern	HKFGK	GV	K	VII.3.1

³ AD: Administration, GV: Geschäftsvorfall

⁴ K: Kunde, I: Kreditinstitut

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 12	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente

Nr.	Name	Kennung	Art ³	Sender ⁴	Kapitel
43	Festgeldkonditionen Parameter	HIFGKS	GV	I	VII.3.1
44	Festgeldkonditionen rückmelden	HIFGK	GV	I	VII.3.1
45	Festgeldneuanlage	HKFGN	GV	K	VII.3.2
46	Festgeldneuanlage bestätigen	HIFGN	GV	I	VII.3.2
47	Festgeldneuanlage Parameter	HIFGNS	GV	I	VII.3.2
48	Festgeldneuanlage widerrufen	HKFGW	GV	K	VII.3.6
49	Festgeldneuanlage widerrufen Parameter	HIFGWS	GV	I	VII.3.6
50	Festgeldprolongation bestätigen	HIFGP	GV	I	VII.3.4
51	Festgeldprolongation Parameter	HIFGPS	GV	I	VII.3.4
52	Festgeldprolongation widerrufen	HKFPW	GV	K	VII.3.7
53	Festgeldprolongation widerrufen Parameter	HIFPWS	GV	I	VII.3.7
54	Gastmeldung	HKGAM	GV	K	VII.7.1.2
55	Gastmeldung Parameter	HIGAMS	GV	I	VII.7.1.2
56	Identifikation	HKIDN	AD	K	III.3.1.2
57	Informationen anfordern	HKINF	GV	K	VII.7.2.2
58	Informationsanforderung Parameter	HIINFS	GV	I	VII.7.2.2
59	Kommunikationszugang anfordern	HKKOM	GV	K	VIII.7
60	Kommunikationszugang Parameter	HIKOMS	GV	I	VIII.7
61	Kommunikationszugang rückmelden	HIKOM	GV	I	VIII.7
62	Komprimierungsverfahren	HIKPV	AD	I	IV.5
63	Kontoinformation	HIUPD	AD	I	V.3
64	Kontoumsätze anfordern/neue Umsätze	HKKAN	GV	K	VII.2.1.2
65	Kontoumsätze anfordern/Zeitraum	HKKAZ	GV	K	VII.2.1.1
66	Kontoumsätze rückmelden/neue Umsätze	HIKAN	GV	I	VII.2.1.2
67	Kontoumsätze rückmelden/Zeitraum	HIKAZ	GV	I	VII.2.1.1
68	Kontoumsätze/neu Parameter	HIKANS	GV	I	VII.2.1.2
69	Kontoumsätze/Zeitraum Parameter	HIKAZS	GV	I	VII.2.1.1
70	Kreditinstitutsangebote anfordern	HKKIA	GV	K	VII.7.2.1
71	Kreditinstitutsangebote Parameter	HIKIAS	GV	I	VII.7.2.1
72	Kreditinstitutsangebote rückmelden	HIKIA	GV	I	VII.7.2.1
73	Kreditinstitutsmeldung	HIKIM	AD	I	III.3.2.5
74	Kundenmeldung	HKKDM	GV	K	VII.7.1.1
75	Kundenmeldung Parameter	HIKDMS	GV	I	VII.7.1.1
76	Lastschrift Parameter	HILASS	GV	I	VII.1.1.5
77	Nachrichtenabschluß	HNHBS	AD	K/I	II.6.3
78	Nachrichtenkopf	HNHBK	AD	K/I	II.6.2
79	Rückmeldung zu Segmenten	HIRMS	AD	I	II.8.3
80	Rückmeldungen zur Gesamtnachricht	HIRMG	AD	I	II.8.2
81	Saldenabfrage	HKSAL	GV	K	VII.2.2
82	Saldenabfrage Parameter	HISALS	GV	I	VII.2.2
83	Saldenrückmeldung	HISAL	GV	I	VII.2.2
84	Sammellastschrift	HKSLA	GV	K	VII.1.2.2
85	Sammellastschrift Parameter	HISLAS	GV	I	VII.1.2.2
86	Sammelüberweisung	HKSUB	GV	K	VII.1.2.1
87	Sammelüberweisung Parameter	HISUBS	GV	I	VII.1.2.1
88	Schlüsseländerung	HKSAK	AD	K	VI.6.1.1
89	Schlüsselsperrung	HKSSP	AD	K	VI.6.1.4
90	Sicherheitsverfahren	HISHV	AD	I	IV.4
91	Signaturabschluß	HNSHA	AD	K/I	VI.5.3
92	Signaturkopf	HNSHK	AD	K/I	VI.5.2
93	Statusprotokoll anfordern	HKPRO	GV	K	III.7
94	Statusprotokoll Parameter	HIPROS	GV	I	III.7
95	Statusprotokoll rückmelden	HIPRO	GV	I	III.7

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente	Stand: 02.02.1998	Seite: 13

Nr.	Name	Kennung	Art ³	Sender ⁴	Kapitel
96	Synchronisierung	HKSYN	AD	K	III.8.1.2
97	Synchronisierungsantwort	HISYN	AD	I	III.8.2.2
98	Terminierte Überweisung ändern	HKTUA	GV	K	VII.1.1.3.2
99	Terminierte Überweisung ändern Parameter	HITUAS	GV	I	VII.1.1.3.2
100	Terminierte Überweisung einreichen	HKTUE	GV	K	VII.1.1.3.1
101	Terminierte Überweisung einreichen Parameter	HITUES	GV	I	VII.1.1.3.1
102	Terminierte Überweisung löschen	HKTUL	GV	K	VII.1.1.3.4
103	Terminierte Überweisung löschen Parameter	HITULS	GV	I	VII.1.1.3.4
104	Terminvereinbarung	HKTMV	GV	K	VII.7.2.3
105	Terminvereinbarung Parameter	HITMVS	GV	I	VII.7.2.3
106	Übermittlung eines öffentlichen Schlüssels	HIISA	AD	I	VI.6.1.3
107	Userparameter allgemein	HIUPA	AD	I	V.2
108	Verarbeitungsvorbereitung	HKVVB	AD	K	III.3.1.3
109	Verschlüsselte Daten	HNVS	AD	K/I	VI.5.5
110	Verschlüsselungskopf	HNVSK	AD	K/I	VI.5.4
111	Vordruckbestellung	HKVDB	GV	K	VII.6.1.1
112	Vordruckbestellung Parameter	HIVDBS	GV	I	VII.6.1.1

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 14	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente

VIII.2.4 Datenelementgruppen

Nr.	Name	Format
1	Adresse	adr
2	Anlagebetrag	btg
3	Anlagebetrag bis	btg
4	Anlagebetrag neu	btg
5	Anlagebetrag von	btg
6	Anlagekonto	kto
7	Anlagekonto alt	kto
8	Ausbuchungskonto	kto
9	Aussetzung	VII.1.1.4
10	Belastungskonto	kto
11	Bereits verfügbarer Betrag	btg
12	Betrag	btg
13	Bezugsnachricht	II.6.2
14	Dauerauftragdetails	VII.1.1.4
15	Depot	kto
16	Erlaubte Geschäftsvorfälle	V.3
17	Festgeldkondition	VII.3
18	Formular	VII.6.1.1
19	Gebuchter Saldo	sdo
20	Hashalgorithmus	VI.5.2.2
21	Informationen	VII.7.2.1
22	Informationscodes	VII.7.2.2
23	Kommunikationsparameter	VIII.7
24	Kontolimit	V.3
25	Kontoverbindung	kto
26	Kontoverbindung Auftraggeber	kto
27	Kontoverbindung Empfänger/Zahlungspflichtiger	kto
28	Kreditinstitutskennung	kik
29	Kreditlinie	btg
30	Limitbetrag	btg
31	Öffentlicher Schlüssel	VI.5.1.5
32	Parameter	IV.6
33	Parameter Auslandsüberweisung	VII.5.1
34	Parameter Bestand terminierter Überweisungen	VII.1.1.3.3
35	Parameter Dauerauftrag ändern	VII.1.1.4.2
36	Parameter Dauerauftrag aussetzen	VII.1.1.4.3
37	Parameter Dauerauftrag einrichten	VII.1.1.4.1
38	Parameter Dauerauftrag löschen	VII.1.1.4.6
39	Parameter Depotaufstellung	VII.4.1
40	Parameter Einzelüberweisung/-lastschrift	VII.1.1.1
41	Parameter Festgeld ändern	VII.3.3
42	Parameter Festgeldkonditionen	VII.3.1
43	Parameter Festgeldneuanlage	VII.3.2
44	Parameter Kontoumsätze	VII.2.1.1
45	Parameter Kunden-/Gastmeldung	VII.7.1.1
46	Parameter Sammelüberweisung/-lastschrift	VII.1.2.1
47	Parameter terminierte Überweisung ändern	VII.1.1.3.2
48	Parameter terminierte Überweisung einreichen	VII.1.1.3.1
49	Parameter Vordruckbestellung	VII.6.1.1
50	Prolongation	VII.3
51	Rückmeldung	II.8.5.2

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente	Stand: 02.02.1998	Seite: 15

Nr.	Name	Format
52	Saldo der vorgemerkten Umsätze	sdo
53	Schlüsselname	VI.5.1.1
54	Segmentkopf	II.6.1
55	Sicherheitsdatum und -uhrzeit	VI.5.1.2
56	Sicherheitsidentifikation, Details	VI.5.1.3
57	Signaturalgorithmus	VI.5.2.3
58	Unterstützte HBCI-Versionen	IV.2
59	Unterstützte Komprimierungsverfahren	IV.5
60	Unterstützte Sicherheitsverfahren	IV.4
61	Unterstützte Sprachen	IV.2
62	Verfügbarer Betrag	btg
63	Verschlüsselungsalgorithmus	VI.5.4.2
64	Version der Konditionen	VII.3
65	Verwendungszweck	VII.1.1
66	Zertifikat	VI.5.1.4
67	Zinsertrag voraussichtlich	btg
68	Zinsgutschriftkonto	kto

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 16	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente

VIII.2.5 Datenelemente

Nr.	Name	Format	Länge
1	Ablaufdatum	dat	#
2	Abweichendes Ausbuchungskonto erlaubt	jn	#
3	Abweichendes Zinsgutschriftkonto erlaubt	jn	#
4	Adressaufdruck	jn	#
5	Adressaufdruck möglich	jn	#
6	Alle Konten	jn	#
7	Anlagedatum	dat	#
8	Anzahl Aussetzungen	num	..2
9	Anzahl benötigter Signaturen	num	..2
10	Anzahl Geschäftsvorfällearten	num	..3
11	Anzahl Signaturen mindestens	num	1
12	Anzahl terminierter Änderungen	num	1
13	Anzahl terminierter Aussetzungen	num	1
14	Aufsetzpunkt	an	..35
15	Auftragsidentifikation	an	..99
16	Auftragsidentifikation alt	an	..99
17	Ausbuchungskonto änderbar	jn	#
18	Ausführungsdatum	dat	#
19	Ausführungstag	num	..2
20	Ausführungstag änderbar	jn	#
21	Ausführungstage pro Monat	dig	..64
22	Ausführungstage pro Woche	dig	..7
23	Auslieferung	num	1
24	Aussetzen bis	dat	#
25	Aussetzen von	dat	#
26	Aussetzung jährlich wiederkehrend	jn	#
27	Aussetzung jährlich wiederkehrend erlaubt	jn	#
28	Aussetzungseingabe	num	1
29	Austauschkontrollreferenz	id	#
30	Benutzerkennung	id	#
31	Bereich der Sicherheitsapplikation, kodiert	an	..3
32	Beschreibung	an	..35
33	Betrag änderbar	jn	#
34	Betreff	an	..35
35	Bezeichner für Algorithmusparameter, IV	an	..3
36	Bezeichner für Algorithmusparameter, Schlüssel	an	..3
37	Bezeichner für Exponent	an	..3
38	Bezeichner für Funktionstyp	num	..3
39	Bezeichner für Hashalgorithmusparameter	an	..3
40	Bezeichner für Modulus	an	..3
41	Bezeichner für Sicherheitspartei	an	..3
42	Bezugsdatenelement	an	..7
43	Bezugssegment	num	..3
44	Bis BLZ	num	8
45	Bis Datum	dat	#
46	BPD-Version	num	..3
47	CID	bin	..256
48	Daten, verschlüsselt	bin	..
49	Datum	dat	#
50	Datum der Übermittlung	dat	#

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente	Stand: 02.02.1998	Seite: 17

Nr.	Name	Format	Länge
51	Datum- und Zeitbezeichner, kodiert	an	..3
52	Dialog-ID	id	#
53	Dialogsprache	num	..3
54	DTA-Datensatz	bin	..
55	DTAZV-Datensatz	bin	..
56	Eigene Rechnung	jn	#
57	Eingabe Anzahl Einträge erlaubt	jn	#
58	Empfängernamen änderbar	jn	#
59	Erläuterungen	an	..35
60	Erstes Ausführungsdatum änderbar	jn	#
61	Erstmals ausführen am	dat	#
62	Festgeldstatus	num	1
63	Filterfunktion	an	3
64	Format der Information	an	..3
65	Formularbezeichnung	an	..35
66	Formularcode	num	..2
67	Freitextmeldung	txt	..2048
68	Gebuchte Umsätze	bin	..
69	Geschäftsstelle	an	..35
70	Geschäftsvorfall	an	..6
71	Gewünschte Anzahl	num	..3
72	Hashalgorithmus, kodiert	an	..3
73	HBCI-Version	num	..3
74	Identifizierung der Partei	id	#
75	Informationsart	an	1
76	Informationscode	an	..10
77	Kommunikationsadresse	an	..512
78	Kommunikationsadressenzusatz	an	..512
79	Kommunikationsdienst	num	..2
80	Komprimierungsfunktion	an	..3
81	Komprimierungsversion	num	..3
82	Konditionenbezeichnung	an	..30
83	Konditionenidentifikation	id	#
84	Konditionenversion	an	..10
85	Konto-/Depotnummer	id	#
86	Kontoauszugkennzeichen	num	1
87	Kontoauszugkennzeichen änderbar	jn	#
88	Kontoproduktbezeichnung	an	..30
89	Kontoverbindung Empfänger änderbar	jn	#
90	Kontowährung	cur	#
91	Kontraktreferenz	id	#
92	Kontraktreferenz alt	id	#
93	Kreditinstitutsbezeichnung	an	..60
94	Kreditinstitutscode	an	..30
95	Kunden-ID	id	#
96	Kundenberater	an	..35
97	Kundensystem-ID	id	#
98	Kundensystem-Status	num	1
99	Länderkennzeichen	ctr	#
100	Letztes Ausführungsdatum änderbar	jn	#
101	Letztmals ausführen am	dat	#
102	Limit-Tage	num	..3
103	Limitart	an	1
104	Löschung terminierbar	jn	#

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 18	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente

Nr.	Name	Format	Länge
105	Maximale Anzahl Aufträge	num	..3
106	Maximale Anzahl C-Sätze	num	..4
107	Maximale Anzahl Einträge	num	..4
108	Maximale Anzahl T-Sätze	num	..4
109	Maximale Anzahl Verwendungszweckzeilen	num	..2
110	Maximale Länge	num	..4
111	Maximale Nachrichtengröße	num	..4
112	Maximale Vorlaufzeit	num	..4
113	Minimale Vorlaufzeit	num	..4
114	Mischung zulässig	jn	#
115	MT 571	bin	..
116	Nachrichtenbeziehung, kodiert	num	1
117	Nachrichtengröße	dig	12
118	Nachrichtennummer	num	..4
119	Nachrichtenreferenznummer	num	..4
120	Name 1	an	..35
121	Name 2	an	..35
122	Name Empfänger/Zahlungspflichtiger 1	an	..27
123	Name Empfänger/Zahlungspflichtiger 2	an	..27
124	Nicht gebuchte Umsätze	bin	..
125	Operationsmodus, kodiert	an	..3
126	PLZ/Ort	an	..35
127	Produktbezeichnung	an	..25
128	Produktversion	an	..5
129	Prolongationslaufzeit	num	..3
130	Rolle des Sicherheitslieferanten, kodiert	an	..3
131	Rückmeldungscode	dig	4
132	Rückmeldungsparameter	an	..35
133	Rückmeldungstext	an	..80
134	Schlüsselart	an	1
135	Schlüsselnummer	num	..3
136	Schlüsselversion	num	..3
137	Segmentkennung	an	..6
138	Segmentnummer	num	..3
139	Segmentversion	num	..3
140	Sicherheitsfunktion, kodiert	an	..3
141	Sicherheitskontrollreferenz	an	..14
142	Sicherheitsreferenznummer	num	..16
143	Sicherheitsverfahren, Code	an	3
144	Signaturalgorithmus, kodiert	an	..3
145	Soll-Haben-Kennzeichen	an	1
146	Speicherzeitraum	num	..4
147	Sperrenkennzeichen	an	..3
148	Standardsprache	num	..3
149	Straße/Postfach	an	..35
150	Synchronisierungsmodus	num	1
151	Telefon	an	..35
152	Telefonnummer für Bestätigung	an	..35
153	Textschlüssel	dig	2
154	Textschlüssel und -ergänzung änderbar	jn	#
155	Textschlüsselergänzung	dig	3
156	Thema	an	..200
157	Turnus	num	..2
158	Turnus änderbar	jn	#

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente	Stand: 02.02.1998	Seite: 19

Nr.	Name	Format	Länge
159	Turnus in Monaten	dig	..24
160	Turnus in Wochen	dig	..104
161	Uhrzeit	tim	#
162	Uhrzeit der Übermittlung	tim	#
163	Unterstützte HBCI-Version	num	..3
164	Unterstützte Sprache	num	..3
165	UPD-Version	num	..3
166	UPD-Verwendung	num	1
167	Validierungsergebnis	bin	..512
168	Verfahren Benutzer	an	..3
169	Verschlüsselungsalgorithmus, kodiert	an	..3
170	Version der Filterfunktion	num	..3
171	Version der Information	dat	#
172	Version des Sicherheitsverfahrens	num	..3
173	Verwendung des Hashalgorithmus, kodiert	an	..3
174	Verwendung des Signaturalgorithmus, kodiert	an	..3
175	Verwendung des Verschlüsselungsalgorithmus, kodiert	an	..3
176	Verwendungszweck änderbar	jn	#
177	Verwendungszweck für öffentlichen Schlüssel	an	..3
178	Verwendungszweckzeile	an	..27
179	Von BLZ	num	8
180	Von Datum	dat	#
181	Währung	cur	#
182	Währung der Konditionen	cur	#
183	Wert	wrt	#
184	Wert des Algorithmusparameters, IV	bin	..512
185	Wert des Algorithmusparameters, Schlüssel	bin	..512
186	Wert des Hashalgorithmusparameters	bin	..512
187	Wert für Exponent	bin	..512
188	Wert für Modulus	bin	..512
189	Wiederanlagekennzeichen	num	1
190	Wiederanlagekennzeichen änderbar	jn	#
191	Wiederanlagekennzeichen bei Prolongation	num	1
192	Zeiteinheit	an	1
193	Zeiteinheit änderbar	jn	#
194	Zeitraum möglich	jn	#
195	Zertifikatsinhalt	bin	.. 2048
196	Zertifikatstyp	num	1
197	Zinsgutschriftkonto änderbar	jn	#
198	Zinsmethode	an	1
199	Zinssatz	wrt	#

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 20	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente

VIII.2.6 HBCI-Elemente allgemein

Nr.	Name	Typ ⁵
1	Ablaufdatum	DE
2	Abweichendes Ausbuchungskonto erlaubt	DE
3	Abweichendes Zinsgutschriftkonto erlaubt	DE
4	Adressaufdruck	DE
5	Adressaufdruck möglich	DE
6	Adresse	MVE
7	Adresse	DEG
8	Alle Konten	DE
9	Änderung eines öffentlichen Schlüssels des Kunden	N
10	Änderung terminierter Überweisung bestätigen	SEG
11	Anforderung eines öffentlichen Schlüssels	SEG
12	Anlagebetrag	DEG
13	Anlagebetrag bis	DEG
14	Anlagebetrag neu	DEG
15	Anlagebetrag von	DEG
16	Anlagedatum	DE
17	Anlagekonto	DEG
18	Anlagekonto alt	DEG
19	Antwort auf Dialoginitialisierung	N
20	Antwort auf anonyme Dialoginitialisierung	N
21	Antwort auf Kommunikationszugang	N
22	Anzahl Aussetzungen	DE
23	Anzahl benötigter Signaturen	DE
24	Anzahl Geschäftsvorfallsarten	DE
25	Anzahl Signaturen mindestens	DE
26	Anzahl terminierter Änderungen	DE
27	Anzahl terminierter Aussetzungen	DE
28	Aufsetzpunkt	DE
29	Aufträge	SF
30	Auftragsidentifikation	DE
31	Auftragsidentifikation alt	DE
32	Ausbuchungskonto	DEG
33	Ausbuchungskonto änderbar	DE
34	Ausführungsdatum	DE
35	Ausführungstag	DE
36	Ausführungstag änderbar	DE
37	Ausführungstage pro Monat	DE
38	Ausführungstage pro Woche	DE
39	Auslandsüberweisung	SEG
40	Auslandsüberweisung Parameter	SEG
41	Auslieferung	DE
42	Aussetzen bis	DE
43	Aussetzen von	DE

⁵ DE: Datenelement bzw. Gruppenelement
DEG: Datenelementgruppe bzw. Gruppenelement-Gruppe
MVE: Mehrfach verwendetes Element
N: Nachricht
SEG: Segment
SF: Segmentfolge

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente	Stand: 02.02.1998	Seite: 21

Nr.	Name	Typ ⁵
44	Aussetzung	DEG
45	Aussetzung jährlich wiederkehrend	DE
46	Aussetzung jährlich wiederkehrend erlaubt	DE
47	Aussetzungseingabe	DE
48	Austauschkontrollreferenz	DE
49	Bankparameter allgemein	SEG
50	Bankparameterdaten	SF
51	Belastungskonto	DEG
52	Benutzerkennung	DE
53	Bereich der Sicherheitsapplikation, kodiert	DE
54	Bereits verfügbarer Betrag	DEG
55	Beschreibung	DE
56	Bestand terminierter Überweisungen anfordern	SEG
57	Bestand terminierter Überweisungen Parameter	SEG
58	Bestand terminierter Überweisungen rückmelden	SEG
59	Bestätigung der Schlüsselsperrung	SEG
60	Bestätigung der Schlüsselsperrung durch das Kreditinstitut	N
61	Betrag	MVE
62	Betrag	DEG
63	Betrag änderbar	DE
64	Betreff	DE
65	Bezeichner für Algorithmusparameter, IV	DE
66	Bezeichner für Algorithmusparameter, Schlüssel	DE
67	Bezeichner für Exponent	DE
68	Bezeichner für Funktionstyp	DE
69	Bezeichner für Hashalgorithmusparameter	DE
70	Bezeichner für Modulus	DE
71	Bezeichner für Sicherheitspartei	DE
72	Bezugsdatenelement	DE
73	Bezugsnachricht	DEG
74	Bezugssegment	DE
75	Bis BLZ	DE
76	Bis Datum	DE
77	BPD-Version	DE
78	CID	DE
79	Daten, verschlüsselt	DE
80	Datensegmente	SF
81	Datum	DE
82	Datum der Übermittlung	DE
83	Datum- und Zeitbezeichner, kodiert	DE
84	Dauerauftrag ändern	SEG
85	Dauerauftrag ändern Parameter	SEG
86	Dauerauftrag aussetzen	SEG
87	Dauerauftrag aussetzen Parameter	SEG
88	Dauerauftrag einrichten	SEG
89	Dauerauftrag einrichten Parameter	SEG
90	Dauerauftrag löschen	SEG
91	Dauerauftrag löschen Parameter	SEG
92	Dauerauftragdetails	DEG
93	Dauerauftragsänderung bestätigen	SEG
94	Dauerauftragsänderungsvormerkungen anfordern	SEG
95	Dauerauftragsänderungsvormerkungen Parameter	SEG
96	Dauerauftragsänderungsvormerkungen rückmelden	SEG
97	Dauerauftragsaussetzung bestätigen	SEG

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 22	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente

Nr.	Name	Typ ⁵
98	Dauerauftragsbestand anfordern	SEG
99	Dauerauftragsbestand Parameter	SEG
100	Dauerauftragsbestand rückmelden	SEG
101	Dauerauftragseinrichtung bestätigen	SEG
102	Depot	DEG
103	Depotaufstellung	SEG
104	Depotaufstellung anfordern	SEG
105	Depotaufstellung Parameter	SEG
106	Dialog-ID	DE
107	Dialogbeendigung	N
108	Dialogbeendigung bei anonymem Zugang	N
109	Dialogende	SEG
110	Dialoginitialisierung	N
111	Dialoginitialisierung bei anonymem Zugang	N
112	Dialogsprache	DE
113	DTA-Datensatz	DE
114	DTAZV-Datensatz	DE
115	Eigene Rechnung	DE
116	Eingabe Anzahl Einträge erlaubt	DE
117	Einreichung terminierter Überweisung bestätigen	SEG
118	Einzellastschrift	SEG
119	Einzelüberweisung	SEG
120	Einzelüberweisung Parameter	SEG
121	Empfängername änderbar	DE
122	Erlaubte Geschäftsvorfälle	DEG
123	Erläuterungen	DE
124	Erstes Ausführungsdatum änderbar	DE
125	Erstmalige Anforderung der Schlüssel des Kreditinstituts	N
126	Erstmalige Übermittlung der Schlüssel des Kreditinstituts	N
127	Erstmalige Übermittlung der Schlüssel des Kunden	N
128	Erstmals ausführen am	DE
129	Festgeld ändern Parameter	SEG
130	Festgeldänderung bestätigen	SEG
131	Festgeldanlage ändern	SEG
132	Festgeldanlage prolongieren	SEG
133	Festgeldbestand anfordern	SEG
134	Festgeldbestand Parameter	SEG
135	Festgeldbestand rückmelden	SEG
136	Festgeldkondition	DEG
137	Festgeldkonditionen anfordern	SEG
138	Festgeldkonditionen Parameter	SEG
139	Festgeldkonditionen rückmelden	SEG
140	Festgeldneuanlage	SEG
141	Festgeldneuanlage bestätigen	SEG
142	Festgeldneuanlage Parameter	SEG
143	Festgeldneuanlage widerrufen	SEG
144	Festgeldneuanlage widerrufen Parameter	SEG
145	Festgeldprolongation bestätigen	SEG
146	Festgeldprolongation Parameter	SEG
147	Festgeldprolongation widerrufen	SEG
148	Festgeldprolongation widerrufen Parameter	SEG
149	Festgeldstatus	DE
150	Filterfunktion	DE
151	Format der Information	DE

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente	Stand: 02.02.1998	Seite: 23

Nr.	Name	Typ ⁵
152	Formular	DEG
153	Formularbezeichnung	DE
154	Formularcode	DE
155	Freitextmeldung	DE
156	Gastmeldung	SEG
157	Gastmeldung Parameter	SEG
158	Gebuchte Umsätze	DE
159	Gebuchter Saldo	DEG
160	Geschäftsstelle	DE
161	Geschäftsvorfall	DE
162	Gewünschte Anzahl	DE
163	Hashalgorithmus	DEG
164	Hashalgorithmus, kodiert	DE
165	HBCI-Version	DE
166	Identifikation	SEG
167	Identifizierung der Partei	DE
168	Informationen	DEG
169	Informationen anfordern	SEG
170	Informationsanforderung Parameter	SEG
171	Informationsart	DE
172	Informationscode	DE
173	Informationscodes	DEG
174	Kommunikationsadresse	DE
175	Kommunikationsadressenzusatz	DE
176	Kommunikationsdienst	DE
177	Kommunikationsparameter	DEG
178	Kommunikationszugang	N
179	Kommunikationszugang anfordern	SEG
180	Kommunikationszugang Parameter	SEG
181	Kommunikationszugang rückmelden	SEG
182	Komprimierungsfunktion	DE
183	Komprimierungsverfahren	SEG
184	Komprimierungsversion	DE
185	Konditionenbezeichnung	DE
186	Konditionenidentifikation	DE
187	Konditionenversion	DE
188	Konto-/Depotnummer	DE
189	Kontoauszugkennzeichen	DE
190	Kontoauszugkennzeichen änderbar	DE
191	Kontoinformation	SEG
192	Kontolimit	DEG
193	Kontoproduktbezeichnung	DE
194	Kontoumsätze anfordern/neue Umsätze	SEG
195	Kontoumsätze anfordern/Zeitraum	SEG
196	Kontoumsätze rückmelden/neue Umsätze	SEG
197	Kontoumsätze rückmelden/Zeitraum	SEG
198	Kontoumsätze/neu Parameter	SEG
199	Kontoumsätze/Zeitraum Parameter	SEG
200	Kontoverbindung	DEG
201	Kontoverbindung	MVE
202	Kontoverbindung Auftraggeber	DEG
203	Kontoverbindung Empfänger änderbar	DE
204	Kontoverbindung Empfänger/Zahlungspflichtiger	DEG
205	Kontowährung	DE

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 24	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente

Nr.	Name	Typ ⁵
206	Kontraktreferenz	DE
207	Kontraktreferenz alt	DE
208	Kreditinstitutsangebote anfordern	SEG
209	Kreditinstitutsangebote Parameter	SEG
210	Kreditinstitutsangebote rückmelden	SEG
211	Kreditinstitutsbezeichnung	DE
212	Kreditinstitutscode	DE
213	Kreditinstitutskennung	DEG
214	Kreditinstitutskennung	MVE
215	Kreditinstitutsmeldung	SEG
216	Kreditinstitutsnachricht allgemein	N
217	Kreditlinie	DEG
218	Kunden-ID	DE
219	Kundenberater	DE
220	Kundenmeldung	SEG
221	Kundenmeldung Parameter	SEG
222	Kundennachricht allgemein	N
223	Kundennachricht allgemein bei anonymem Zugang	N
224	Kundensystem-ID	DE
225	Kundensystem-Status	DE
226	Länderkennzeichen	DE
227	Lastschrift Parameter	SEG
228	Letztes Ausführungsdatum änderbar	DE
229	Letztmals ausführen am	DE
230	Limit-Tage	DE
231	Limitart	DE
232	Limitbetrag	DEG
233	Löschung terminierbar	DE
234	Maximale Anzahl Aufträge	DE
235	Maximale Anzahl C-Sätze	DE
236	Maximale Anzahl Einträge	DE
237	Maximale Anzahl T-Sätze	DE
238	Maximale Anzahl Verwendungszweckzeilen	DE
239	Maximale Länge	DE
240	Maximale Nachrichtengröße	DE
241	Maximale Vorlaufzeit	DE
242	Minimale Vorlaufzeit	DE
243	Mischung zulässig	DE
244	MT 571	DE
245	Nachrichtenabschluß	SEG
246	Nachrichtenbeziehung, kodiert	DE
247	Nachrichtengröße	DE
248	Nachrichtenkopf	SEG
249	Nachrichtennummer	DE
250	Nachrichtenreferenznummer	DE
251	Name 1	DE
252	Name 2	DE
253	Name Empfänger/Zahlungspflichtiger 1	DE
254	Name Empfänger/Zahlungspflichtiger 2	DE
255	Nicht gebuchte Umsätze	DE
256	Öffentlicher Schlüssel	DEG
257	Operationsmodus, kodiert	DE
258	Parameter	DEG
259	Parameter Auslandsüberweisung	DEG

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente	Stand: 02.02.1998	Seite: 25

Nr.	Name	Typ ⁵
260	Parameter Bestand terminierter Überweisungen	DEG
261	Parameter Dauerauftrag ändern	DEG
262	Parameter Dauerauftrag aussetzen	DEG
263	Parameter Dauerauftrag einrichten	DEG
264	Parameter Dauerauftrag löschen	DEG
265	Parameter Depotaufstellung	DEG
266	Parameter Einzelüberweisung/-lastschrift	DEG
267	Parameter Festgeld ändern	DEG
268	Parameter Festgeldkonditionen	DEG
269	Parameter Festgeldneuanlage	DEG
270	Parameter Kontoumsätze	DEG
271	Parameter Kunden-/Gastmeldung	DEG
272	Parameter Sammelüberweisung/-lastschrift	DEG
273	Parameter terminierte Überweisung ändern	DEG
274	Parameter terminierte Überweisung einreichen	DEG
275	Parameter Vordruckbestellung	DEG
276	Parameterdaten	SF
277	PLZ/Ort	DE
278	Produktbezeichnung	DE
279	Produktversion	DE
280	Prolongation	DEG
281	Prolongationslaufzeit	DE
282	Rolle des Sicherheitslieferanten, kodiert	DE
283	Rückmeldung	DEG
284	Rückmeldung zu Segmenten	SEG
285	Rückmeldungen zur Gesamtnachricht	SEG
286	Rückmeldungscode	DE
287	Rückmeldungsparameter	DE
288	Rückmeldungstext	DE
289	Saldenabfrage	SEG
290	Saldenabfrage Parameter	SEG
291	Saldenrückmeldung	SEG
292	Saldo	MVE
293	Saldo der vorgemerkten Umsätze	DEG
294	Sammellastschrift	SEG
295	Sammellastschrift Parameter	SEG
296	Sammelüberweisung	SEG
297	Sammelüberweisung Parameter	SEG
298	Schlüsseländerung	SEG
299	Schlüsselart	DE
300	Schlüsselname	DEG
301	Schlüsselnummer	DE
302	Schlüsselsperrung	SEG
303	Schlüsselversion	DE
304	Segmentkennung	DE
305	Segmentkopf	DEG
306	Segmentnummer	DE
307	Segmentversion	DE
308	Sicherheitsdatum und -uhrzeit	DEG
309	Sicherheitsfunktion, kodiert	DE
310	Sicherheitsidentifikation, Details	DEG
311	Sicherheitskontrollreferenz	DE
312	Sicherheitsreferenznummer	DE
313	Sicherheitsverfahren	SEG

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 26	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente

Nr.	Name	Typ ⁵
314	Sicherheitsverfahren, Code	DE
315	Signaturabschluß	SEG
316	Signaturalgorithmus	DEG
317	Signaturalgorithmus, kodiert	DE
318	Signaturkopf	SEG
319	Soll-Haben-Kennzeichen	DE
320	Speicherzeitraum	DE
321	Sperrenkennzeichen	DE
322	Sperrung eines Schlüssels durch den Kunden	N
323	Standardsprache	DE
324	Statusprotokoll anfordern	SEG
325	Statusprotokoll Parameter	SEG
326	Statusprotokoll rückmelden	SEG
327	Straße/Postfach	DE
328	Synchronisierung	SEG
329	Synchronisierungsantwort	SEG
330	Synchronisierungsantwortnachricht	N
331	Synchronisierungsmodus	DE
332	Synchronisierungsnachricht	N
333	Telefon	DE
334	Telefonnummer für Bestätigung	DE
335	Terminierte Überweisung ändern	SEG
336	Terminierte Überweisung ändern Parameter	SEG
337	Terminierte Überweisung einreichen	SEG
338	Terminierte Überweisung einreichen Parameter	SEG
339	Terminierte Überweisung löschen	SEG
340	Terminierte Überweisung löschen Parameter	SEG
341	Terminvereinbarung	SEG
342	Terminvereinbarung Parameter	SEG
343	Textschlüssel	DE
344	Textschlüssel und -ergänzung änderbar	DE
345	Textschlüsselergänzung	DE
346	Thema	DE
347	Turnus	DE
348	Turnus änderbar	DE
349	Turnus in Monaten	DE
350	Turnus in Wochen	DE
351	Übermittlung eines öffentlichen Schlüssels	SEG
352	Uhrzeit	DE
353	Uhrzeit der Übermittlung	DE
354	Unterstützte HBCI-Version	DE
355	Unterstützte HBCI-Versionen	DEG
356	Unterstützte Komprimierungsverfahren	DEG
357	Unterstützte Sicherheitsverfahren	DEG
358	Unterstützte Sprache	DE
359	Unterstützte Sprachen	DEG
360	UPD-Version	DE
361	UPD-Verwendung	DE
362	Userparameter allgemein	SEG
363	Userparameterdaten	SF
364	Validierungsergebnis	DE
365	Verarbeitungsvorbereitung	SEG
366	Verfahren Benutzer	DE
367	Verfügbarer Betrag	DEG

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht der HBCI-Elemente	Stand: 02.02.1998	Seite: 27

Nr.	Name	Typ ⁵
368	Verschlüsselte Daten	SEG
369	Verschlüsselte Nachricht	N
370	Verschlüsselungsalgorithmus	DEG
371	Verschlüsselungsalgorithmus, kodiert	DE
372	Verschlüsselungskopf	SEG
373	Version der Filterfunktion	DE
374	Version der Information	DE
375	Version der Konditionen	DEG
376	Version des Sicherheitsverfahrens	DE
377	Verwendung des Hashalgorithmus, kodiert	DE
378	Verwendung des Signaturalgorithmus, kodiert	DE
379	Verwendung des Verschlüsselungsalgorithmus, kodiert	DE
380	Verwendungszweck	DEG
381	Verwendungszweck änderbar	DE
382	Verwendungszweck für öffentlichen Schlüssel	DE
383	Verwendungszweckzeile	DE
384	Von BLZ	DE
385	Von Datum	DE
386	Vordruckbestellung	SEG
387	Vordruckbestellung Parameter	SEG
388	Währung	DE
389	Währung der Konditionen	DE
390	Wert	DE
391	Wert des Algorithmusparameters, IV	DE
392	Wert des Algorithmusparameters, Schlüssel	DE
393	Wert des Hashalgorithmusparameters	DE
394	Wert für Exponent	DE
395	Wert für Modulus	DE
396	Wiederanlagekennzeichen	DE
397	Wiederanlagekennzeichen änderbar	DE
398	Wiederanlagekennzeichen bei Prolongation	DE
399	Zeiteinheit	DE
400	Zeiteinheit änderbar	DE
401	Zeitraum möglich	DE
402	Zertifikat	DEG
403	Zertifikatsinhalt	DE
404	Zertifikatstyp	DE
405	Zinsertrag voraussichtlich	DEG
406	Zinsgutschriftkonto	DEG
407	Zinsgutschriftkonto änderbar	DE
408	Zinsmethode	DE
409	Zinssatz	DE

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht Nachrichtenaufbau	Stand: 02.02.1998	Seite: 29

VIII.3 Übersicht Nachrichtenaufbau

In den Tabellen ist zu den folgenden Dialogtypen jeweils die Reihenfolge und Anzahl der möglichen Nachrichten und Segmente dargestellt:

- Standarddialog
- Anonymer Dialog
- Synchronisierung
- Kommunikationszugänge abholen
- Änderung eines öffentlichen Schlüssels des Kunden
- Erstmalige Anforderung der öffentlichen Schlüssel des Kreditinstituts
- Erstmalige Übermittlung der öffentlichen Schlüssel des Kunden
- Schlüsselsperrung durch den Kunden

Alle Darstellungen beziehen sich auf den unverschlüsselten Aufbau. Zusätzlich ist daher das allgemeine Format für verschlüsselte Nachrichten angegeben.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 30	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht Nachrichtenaufbau

VIII.3.1 Standarddialog

Segment	Nachricht					
	Dialoginitialisierung		Auftragsnachricht		Dialogbeendigung	
	Kunde	Kredit-institut	Kunde	Kredit-institut	Kunde	Kredit-institut
	N6	N2	N15	N14	N8	N14
Nachricht	1	1	0-n	0-n	1	1
HNHBK	1	1	1	1	1	1
HNSHK	1	0-1	1-3	0-1	1	0-1
HIRMG	-	1	-	1	-	1
HIRMS	-	0-m ¹	-	0-m	-	0-m
HKIDN	1	-	-	-	-	-
HKVVB	1	-	-	-	-	-
HKISA	0/0-2 ²	-	-	-	-	-
HKSYN	-	-	-	-	-	-
HIBPA	-	0-1	-	-	-	-
HIKOM	-	0-1	-	-	-	-
HISHV	-	0-1	-	-	-	-
HIKPV	-	0-1	-	-	-	-
HIUEBS	-	0-n	-	-	-	-
... ³	-	0-n	-	-	-	-
HIUPA	-	0-1	-	-	-	-
HIUPD	-	0-n	-	-	-	-
HIISA	-	0/0-2	-	-	-	-
HISYN	-	-	-	-	-	-
HIKIM	-	0-n	-	-	-	-
HKSAL ⁴	-	-	1	-	-	-
HISAL	-	-	-	0-1	-	-
...	-	-	-	-	-	-
HKPRO	-	-	0-1	-	-	-
HIPRO	-	-	-	0-n	-	-
HKSAK	-	-	-	-	-	-
HKSSP	-	-	-	-	-	-
HISSP	-	-	-	-	-	-
HKKOM	-	-	-	-	-	-
HIKOM	-	-	-	-	-	-
HKEND	-	-	-	-	1	-
HNSHA	1	0-1	1-3	0-1	1	0-1
HNHBS	1	1	1	1	1	1

¹ m: Summe der Segmente der Kundennachricht

² Die Schreibweise 'n/m' bedeutet: n gilt für symmetrische und m für asymmetrische Verfahren.

³ Hier sind für die weiteren unterstützten Geschäftsvorfälle die entsprechenden Parameter-Segmente einzustellen.

⁴ Aus der Gruppe der Auftragssegmente darf z.Zt. nur eine Geschäftsvorfallsart pro Nachricht eingestellt werden. Exemplarisch wird hier der Geschäftsvorfall „Saldenabfrage“ angenommen.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht Nachrichtenaufbau	Stand: 02.02.1998	Seite: 31

VIII.3.2 Anonymer Dialog

Segment	Nachricht					
	Dialoginitialisierung		Auftragsnachricht		Dialogbeendigung	
	Kunde	Kreditinstitut	Kunde	Kreditinstitut	Kunde	Kreditinstitut
	N7	N3	N16	N14	N9	N14
Nachricht	1	1	0-n	0-n	1	1
HNHBK	1	1	1	1	1	1
HNSHK	-	-	-	-	-	-
HIRMG	-	1	-	1	-	1
HIRMS	-	0-m	-	0-m	-	0-m
HKIDN	1	-	-	-	-	-
HKVVB	1	-	-	-	-	-
HKISA	-	-	-	-	-	-
HKSYN	-	-	-	-	-	-
HIBPA	-	0-1	-	-	-	-
HIKOM	-	0-1	-	-	-	-
HISHV	-	0-1	-	-	-	-
HIKPV	-	0-1	-	-	-	-
HIUEBS	-	0-n	-	-	-	-
...	-	0-n	-	-	-	-
HIUPA	-	0-1	-	-	-	-
HIUPD	-	0-n	-	-	-	-
HIISA	-	-	-	-	-	-
HISYN	-	-	-	-	-	-
HIKIM	-	0-n	-	-	-	-
HKSAL ⁵	-	-	-	-	-	-
HISAL	-	-	-	-	-	-
...	-	-	0-n	0-n	-	-
HKPRO	-	-	-	-	-	-
HIPRO	-	-	-	-	-	-
HKSAK	-	-	-	-	-	-
HKSSP	-	-	-	-	-	-
HISSP	-	-	-	-	-	-
HKKOM	-	-	-	-	-	-
HIKOM	-	-	-	-	-	-
HKEND	-	-	-	-	1	-
HNSHA	-	-	-	-	-	-
HNHBS	1	1	1	1	1	1

⁵ Der Kunde kann hier nicht-signierungspflichtige Auftragssegmente senden. Diese Geschäftsvorfälle teilt das Kreditinstitut dem anonymen Kunden in der Gast-UPD mit.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 32	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht Nachrichtenaufbau

VIII.3.3 Synchronisierung

Segment	Nachricht					
	Dialoginitialisierung		Auftragsnachricht		Dialogbeendigung	
	Kunde	Kredit- institut	Kunde	Kredit- institut	Kunde	Kredit- institut
	N18	N19			N8	N14
Nachricht	1	1	0	0	1	1
HNHBK	1	1	-	-	1	1
HNSHK	1	0-1	-	-	1	0-1
HIRMG	-	1	-	-	-	1
HIRMS	-	0-m	-	-	-	0-m
HKIDN	1	-	-	-	-	-
HKVVB	1	-	-	-	-	-
HKISA	0/0-2	-	-	-	-	-
HKSYN	1	-	-	-	-	-
HIBPA	-	0-1	-	-	-	-
HIKOM	-	0-1	-	-	-	-
HISHV	-	0-1	-	-	-	-
HIKPV	-	0-1	-	-	-	-
HIUEBS	-	0-n	-	-	-	-
...	-	0-n	-	-	-	-
HIUPA	-	0-1	-	-	-	-
HIUPD	-	0-n	-	-	-	-
HIISA	-	0/0-2	-	-	-	-
HISYN	-	1	-	-	-	-
HIKIM	-	0-n	-	-	-	-
HKSAL	-	-	-	-	-	-
HISAL	-	-	-	-	-	-
...	-	-	-	-	-	-
HKPRO	-	-	-	-	-	-
HIPRO	-	-	-	-	-	-
HKSAK	-	-	-	-	-	-
HKSSP	-	-	-	-	-	-
HISSP	-	-	-	-	-	-
HKKOM	-	-	-	-	-	-
HIKOM	-	-	-	-	-	-
HKEND	-	-	-	-	1	-
HNSHA	1	0-1	-	-	1	0-1
HNHBS	1	1	-	-	1	1

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht Nachrichtenaufbau	Stand: 02.02.1998	Seite: 33

VIII.3.4 Kommunikationszugang

Segment	Nachricht					
	Dialoginitialisierung		Auftragsnachricht		Dialogbeendigung	
	Kunde	Kredit-institut	Kunde	Kredit-institut	Kunde	Kredit-institut
	N7	N3	N13	N4	N9	N14
Nachricht	1	1	1	1	1	1
HNHBK	1	1	1	1	1	1
HNSHK	-	-	-	-	-	-
HIRMG	-	1	-	1	-	1
HIRMS	-	0-m	-	0-m	-	0-m
HKIDN	1	-	-	-	-	-
HKVVB	1	-	-	-	-	-
HKISA	-	-	-	-	-	-
HKSYN	-	-	-	-	-	-
HIBPA	-	0-1	-	-	-	-
HIKOM	-	0-1	-	-	-	-
HISHV	-	0-1	-	-	-	-
HIKPV	-	0-1	-	-	-	-
HIUEBS	-	0-n	-	-	-	-
...	-	0-n	-	-	-	-
HIUPA	-	0-1	-	-	-	-
HIUPD	-	0-n	-	-	-	-
HIISA	-	-	-	-	-	-
HISYN	-	-	-	-	-	-
HIKIM	-	-	-	-	-	-
HKSAL	-	-	-	-	-	-
HISAL	-	-	-	-	-	-
...	-	-	-	-	-	-
HKPRO	-	-	-	-	-	-
HIPRO	-	-	-	-	-	-
HKSAK	-	-	-	-	-	-
HKSSP	-	-	-	-	-	-
HISSP	-	-	-	-	-	-
HKKOM	-	-	1	-	-	-
HIKOM	-	-	-	0-n	-	-
HKEND	-	-	-	-	1	-
HNSHA	-	-	-	-	-	-
HNHBS	1	1	1	1	1	1

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 34	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht Nachrichtenaufbau

VIII.3.5 Änderung eines öffentlichen Schlüssels des Kunden

Segment	Nachricht					
	Dialoginitialisierung		Auftragsnachricht		Dialogbeendigung	
	Kunde	Kredit- institut	Kunde	Kredit- institut	Kunde	Kredit- institut
	N6	N2	N1	N14	N8	N14
Nachricht	1	1	1	1	1	1
HNHBK	1	1	1	1	1	1
HNSHK	1	0-1	1	0-1	1	0-1
HIRMG	-	1	-	1	-	1
HIRMS	-	0-m	-	0-m	-	0-m
HKIDN	1	-	-	-	-	-
HKVVB	1	-	-	-	-	-
HKISA	0/0-2	-	-	-	-	-
HKSYN	-	-	-	-	-	-
HIBPA	-	0-1	-	-	-	-
HIKOM	-	0-1	-	-	-	-
HISHV	-	0-1	-	-	-	-
HIKPV	-	0-1	-	-	-	-
HIUEBS	-	0-n	-	-	-	-
...	-	0-n	-	-	-	-
HIUPA	-	0-1	-	-	-	-
HIUPD	-	0-n	-	-	-	-
HIISA	-	0/0-2	-	-	-	-
HISYN	-	-	-	-	-	-
HIKIM	-	0-n	-	-	-	-
HKSAL	-	-	-	-	-	-
HISAL	-	-	-	-	-	-
...	-	-	-	-	-	-
HKPRO	-	-	-	-	-	-
HIPRO	-	-	-	-	-	-
HKSAK	-	-	1-2	-	-	-
HKSSP	-	-	-	-	-	-
HISSP	-	-	-	-	-	-
HKKOM	-	-	-	-	-	-
HIKOM	-	-	-	-	-	-
HKEND	-	-	-	-	1	-
HNSHA	1	0-1	1	0-1	1	0-1
HNHBS	1	1	1	1	1	1

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht Nachrichtenaufbau	Stand: 02.02.1998	Seite: 35

VIII.3.6 Erstmalige Anforderung der öffentlichen Schlüssel des Kreditinstituts

Segment	Nachricht					
	Dialoginitialisierung		Auftragsnachricht		Dialogbeendigung	
	Kunde	Kredit-institut	Kunde	Kredit-institut	Kunde	Kredit-institut
	N10	N11			N9	N14
Nachricht	1	1	0	0	1	1
HNHBK	1	1	-	-	1	1
HNSHK	-	0-1	-	-	-	0-1
HIRMG	-	1	-	-	-	1
HIRMS	-	0-m	-	-	-	0-m
HKIDN	1	-	-	-	-	-
HKVVB	1	-	-	-	-	-
HKISA	2	-	-	-	-	-
HKSYN	-	-	-	-	-	-
HIBPA	-	0-1	-	-	-	-
HIKOM	-	0-1	-	-	-	-
HISHV	-	0-1	-	-	-	-
HIKPV	-	0-1	-	-	-	-
HIUEBS	-	0-n	-	-	-	-
...	-	0-n	-	-	-	-
HIUPA	-	-	-	-	-	-
HIUPD	-	-	-	-	-	-
HIISA	-	1-2	-	-	-	-
HISYN	-	-	-	-	-	-
HIKIM	-	-	-	-	-	-
HKSAL	-	-	-	-	-	-
HISAL	-	-	-	-	-	-
...	-	-	-	-	-	-
HKPRO	-	-	-	-	-	-
HIPRO	-	-	-	-	-	-
HKSAK	-	-	-	-	-	-
HKSSP	-	-	-	-	-	-
HISSP	-	-	-	-	-	-
HKKOM	-	-	-	-	-	-
HIKOM	-	-	-	-	-	-
HKEND	-	-	-	-	1	-
HNSHA	-	0-1	-	-	-	0-1
HNHBS	1	1	-	-	1	1

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 36	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht Nachrichtenaufbau

VIII.3.7 Erstmalige Übermittlung der öffentlichen Schlüssel des Kunden

Segment	Nachricht					
	Dialoginitialisierung		Auftragsnachricht		Dialogbeendigung	
	Kunde	Kredit-institut	Kunde	Kredit-institut	Kunde	Kredit-institut
	N12	N14			N8	N14
Nachricht	1	1	0	0	1	1
HNHBK	1	1	-	-	1	1
HNSHK	1	0-1	-	-	1	0-1
HIRMG	-	1	-	-	-	1
HIRMS	-	0-m	-	-	-	0-m
HKIDN	1	-	-	-	-	-
HKVVB	-	-	-	-	-	-
HKISA	-	-	-	-	-	-
HKSYN	-	-	-	-	-	-
HIBPA	-	-	-	-	-	-
HIKOM	-	-	-	-	-	-
HISHV	-	-	-	-	-	-
HIKPV	-	-	-	-	-	-
HIUEBS	-	-	-	-	-	-
...	-	-	-	-	-	-
HIUPA	-	-	-	-	-	-
HIUPD	-	-	-	-	-	-
HIISA	-	-	-	-	-	-
HISYN	-	-	-	-	-	-
HIKIM	-	-	-	-	-	-
HKSAL	-	-	-	-	-	-
HISAL	-	-	-	-	-	-
...	-	-	-	-	-	-
HKPRO	-	-	-	-	-	-
HIPRO	-	-	-	-	-	-
HKSAK	2	-	-	-	-	-
HKSSP	-	-	-	-	-	-
HISSP	-	-	-	-	-	-
HKKOM	-	-	-	-	-	-
HIKOM	-	-	-	-	-	-
HKEND	-	-	-	-	1	-
HNSHA	1	0-1	-	-	1	0-1
HNHBS	1	1	-	-	1	1

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Übersicht Nachrichtenaufbau	Stand: 02.02.1998	Seite: 37

VIII.3.8 Schlüsselsperrung durch den Kunden

Segment	Nachricht					
	Dialoginitialisierung		Auftragsnachricht		Dialogbeendigung	
	Kunde	Kredit- institut	Kunde	Kredit- institut	Kunde	Kredit- institut
	N6, N7	N2, N3	N17	N5	N8, N9	N14
Nachricht	1	1	1	1	1	1
HNHBK	1	1	1	1	1	1
HNSHK	0-1	0-1	0-1	0-1	0-1	0-1
HIRMG	-	1	-	1	-	1
HIRMS	-	0-m	-	0-m	-	0-m
HKIDN	1	-	-	-	-	-
HKVVB	1	-	-	-	-	-
HKISA	0/0-2	-	-	-	-	-
HKSYN	-	-	-	-	-	-
HIBPA	-	0-1	-	-	-	-
HIKOM	-	0-1	-	-	-	-
HISHV	-	0-1	-	-	-	-
HIKPV	-	0-1	-	-	-	-
HIUEBS	-	0-n	-	-	-	-
...	-	0-n	-	-	-	-
HIUPA	-	0-1	-	-	-	-
HIUPD	-	0-n	-	-	-	-
HIISA	-	0/0-2	-	-	-	-
HISYN	-	-	-	-	-	-
HIKIM	-	0-n	-	-	-	-
HKSAL	-	-	-	-	-	-
HISAL	-	-	-	-	-	-
...	-	-	-	-	-	-
HKPRO	-	-	-	-	-	-
HIPRO	-	-	-	-	-	-
HKSAK	-	-	-	-	-	-
HKSSP	-	-	1	-	-	-
HISSP	-	-	-	1	-	-
HKKOM	-	-	-	-	-	-
HIKOM	-	-	-	-	-	-
HKEND	-	-	-	-	1	-
HNSHA	0-1	0-1	0-1	0-1	0-1	0-1
HNHBS	1	1	1	1	1	1

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 38	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Übersicht Nachrichtenaufbau

VIII.3.9 Verschlüsselter Dialog

Segment	Nachricht					
	Dialoginitialisierung		Auftragsnachricht		Dialogbeendigung	
	Kunde	Kredit-institut	Kunde	Kredit-institut	Kunde	Kredit-institut
	N20	N20	N20	N20	N20	N20
Nachricht	1	1	0-n	0-n	1	1
HNHBK	1	1	1	1	1	1
HNVSK	1	1	1	1	1	1
HNVSD	1	1	1	1	1	1
HNHBS	1	1	1	1	1	1

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: HBCI-Basiszeichensätze	Stand: 02.02.1998	Seite: 39

VIII.4 HBCI-Basiszeichensätze

Die HBCI-Basiszeichensätze sind Subsets des ISO 8859. Erlaubt sind nur druckbare Zeichen des ISO 8859-Zeichensatzes, d.h. die Bereiche X'20' bis X'7E' und X'A1' bis X'FF' sowie zusätzlich die Zeichen X'0A' (line feed) und X'0D' (carriage return):

VIII.4.1 ISO 8859-1 Subset Deutsch

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0											LF			CR		
1																
2	SP	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	
8																
9																
A		ı	ø	£	¤	¥	ı	§	¨	©	ª	«	¬	-	®	¯
B	°	±	²	³	´	µ	¶	·	¸	¹	º	»	¼	½	¾	¿
C	À	Á	Â	Ã	Ä	Å	Æ	Ç	È	É	Ê	Ë	Ì	Í	Î	Ï
D	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	×	Ø	Ù	Ú	Û	Ü	Ý	Þ	ß
E	à	á	â	ã	ä	å	æ	ç	è	é	ê	ë	ì	í	î	ï
F	ð	ñ	ò	ó	ô	õ	ö	÷	ø	ù	ú	û	ü	ý	þ	ÿ

VIII.4.2 ISO 8859-1 Subset Englisch

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0											LF			CR		
1																
2	SP	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	
8																
9																
A		ı	ø	£	¤	¥	ı	§	¨	©	ª	«	¬	-	®	¯
B	°	±	²	³	´	µ	¶	·	¸	¹	º	»	¼	½	¾	¿
C	À	Á	Â	Ã	Ä	Å	Æ	Ç	È	É	Ê	Ë	Ì	Í	Î	Ï
D	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	×	Ø	Ù	Ú	Û	Ü	Ý	Þ	ß
E	à	á	â	ã	ä	å	æ	ç	è	é	ê	ë	ì	í	î	ï
F	ð	ñ	ò	ó	ô	õ	ö	÷	ø	ù	ú	û	ü	ý	þ	ÿ

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 40	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: HBCI-Basiszeichensätze

VIII.4.3 ISO 8859-1 Subset Französisch

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0											LF			CR		
1																
2	SP	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	
8																
9																
A		ı	ø	£	¤	¥	ı	§	"	©	ª	«	¬	-	®	-
B	°	±	²	³	´	µ	¶	·	¸	¹	º	»	¼	½	¾	¿
C	À	Á	Â	Ã	Ä	Å	Æ	Ç	È	É	Ê	Ë	Ì	Í	Î	Ï
D	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	×	Ø	Ù	Ú	Û	Ü	Ý	Þ	ß
E	à	á	â	ã	ä	å	æ	ç	è	é	ê	ë	ì	í	î	ï
F	ð	ñ	ò	ó	ô	õ	ö	÷	ø	ù	ú	û	ü	ý	þ	ÿ

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Beispieldialog	Stand: 02.02.1998	Seite: 41

VIII.5 Beispieldialog

Im Beispiel arbeitet der Kunde mit einem Sicherheitsmedium, das asymmetrische Sicherheitsverfahren (RDH) unterstützt.

VIII.5.1 Nachricht „Dialoginitialisierung“

a) Kundennachricht

Die Kundennachricht wird von dem Benutzer mit der Kennung '12345' signiert. Um die Lesbarkeit zu erleichtern, wird der unverschlüsselte Aufbau angezeigt.

Segment: Nachrichtenkopf¹

```
HNHBK:1:2+000000000323+201+0+1'
```

Segment: Signaturkopf

```
HNSHK:2:3+1+654321+1+1+1::2+3234+1:19960701:1111  
44+1:999:1+6:10:16+280:10020030:12345:S:1:1'
```

Segment: Identifikation

```
HKIDN:3:2+280:10020030+12345+2+1'
```

Segment: Verarbeitungsvorbereitung

```
HKVVB:4:2+2+3+1+Homebanking Plus+3.0'
```

Segment: Anforderung eines öffentlichen Schlüssels (Signierschlüssel)

```
HKISA:5:2+2+124+280:10020030:12345:S:1:1'
```

Segment: Anforderung eines öffentlichen Schlüssels (Chiffrierschlüssel)

```
HKISA:6:2+2+124+280:10020030:12345:V:1:1'
```

Segment: Signaturabschluß

```
HNSHA:7:1+654321+@96@<Signatur>'
```

Segment: Nachrichtenabschluß

```
HNHBS:8:1+1'
```

¹ Aus Gründen der Übersichtlichkeit beginnen Segmente in diesem Beispiel jeweils in einer neuen Zeile. Dies bedeutet jedoch nicht, daß Segmente syntaktisch mit einem Zeilenvorschub beendet werden.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 42	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Beispieldialog

b) Kreditinstitutsnachricht

Kreditinstitutsnachrichten werden in diesem Beispiel nicht signiert. Der Kunde erhält zusätzlich jeweils die aktuellen Bankparameterdaten, Userparameterdaten und den aktuellen Signierschlüssel.

Segment: Nachrichtenkopf

```
HNHBK:1:2+000000000932+201+4711+1+4711:1'
```

Segment: Rückmeldungen zur Gesamtnachricht

```
HIRMG:2:2+0010::Nachricht entgegengenommen'
```

Segment: Rückmeldungen zu Segmenten

Segmentfolge: Bankparameterdaten

```
HIBPA:3:2:4+3+280:10020030+Musterbank in Musters  
tadt+1+1:2:3+1+100'
```

```
HIKOM:4:2:4+280:10020030+1+1:12345678:00+2:12345  
679:00+3:123.456.789.01::UUE:1'
```

```
HISHV:5:2:4+N+RDH:3:2:1'
```

```
HIUEBS:6:1:4+1+2+7:51:53:54:67:69'
```

```
HIUEBS:7:2:4+1+2+14:51:53:54:67:69'
```

```
HILASS:8:2:4+1+2+14:04:05'
```

```
HISUBS:9:2:4+1+2+999:14:51:53:54'
```

```
HISLAS:10:2:4+1+2+99:14:04:05'
```

```
HIKAZS:11:2:4+1+2+60:J'
```

```
HIKANS:12:2:4+1+2+60:J'
```

```
HISALS:13:3:4+1+2'
```

Segmentfolge: Userparameterdaten

```
HIUPA:14:2:4+12345+4+0'
```

```
HIUPD:15:3:4+1234567:280:10020030+12345+DEM+Erns  
t Müller++Giro Spezial+T:2000,:DEM+HKPRO:1+HKSAK  
:1+HKISA:1+HKSSP:1+HKUEB:1+HKLAS:1+HKKAN:1+HKKAZ  
:1+HKSAL:1'
```

```
HIUPD:16:3:4+1234568:280:10020030+12345+DEM+Erns  
t Müller++Sparkonto 2000++HKPRO:1+HKSAK:0+HKISA:  
1+HKSSP:0+HKUEB:2:Z:1000,:DEM:7+HKKAN:1+HKKAZ:1+  
HKSAL:2'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Beispieldialog	Stand: 02.02.1998	Seite: 43

Segment: Übermittlung eines öffentlichen Schlüssels (Signierschlüssel)

HIISA:17:2:5+1+333+1+224+280:10020030:12345:S:1:
1+6:16:10:@96@<Modulus>:12:@5@<Exponent>:13 '

Segment: Übermittlung eines öffentlichen Schlüssels (Chiffrierschlüssel)²

Segment: Kreditinstitutsmeldung

HIKIM:18:2+Bausparförderung+Informieren Sie sich
über die neue Bausparförderung. '

Segment: Nachrichtenabschluß

HNHBS:19:1+1 '

² Es wird angenommen, daß der öffentliche Chiffrierschlüssel noch aktuell ist, und daher nicht aktualisiert werden muß.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 44	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Beispieldialog

VIII.5.2 Nachricht „Einzelüberweisung“

a) Kundennachricht

Diese Nachricht wird sowohl von Benutzer '12345' als auch von Benutzer '76543' signiert.

Segment: Nachrichtenkopf

```
HNHBK:1:2+000000000523+201+4711+2'
```

Segment: Signaturkopf für Benutzer '76543'

```
HNSHK:2:3+1+765432+1+1+1::2+3234+1:19960701:1111  
44+1:999:1+6:10:16+280:10020030:76543:S:1:1'
```

Segment: Signaturkopf für Benutzer '12345'

```
HNSHK:3:2+1+654321+1+1+1::2+3234+1:19960701:1111  
44+1:999:1+6:10:16+280:10020030:12345:S:1:1'
```

Segment: Einzelüberweisung

```
HKUEB:4:2+1234567:280:10020030+7654321:280:20030  
040+MEIER FRANZ++1000,:DEM+51+000+RE-NR.1234:KD-  
NR.9876'
```

Segment: Signaturabschluß für Benutzer '12345'

```
HNSHA:5:1+654321+@96@<Signatur>'
```

Segment: Signaturabschluß für Benutzer '76543'

```
HNSHA:6:1+765432+@96@<Signatur>'
```

Segment: Nachrichtenabschluß

```
HNHBS:7:1+2'
```

b) Kreditinstitutsnachricht

Segment: Nachrichtenkopf

```
HNHBK:1:2+000000000140+201+4711+2+4711:2'
```

Segment: Rückmeldungen zur Gesamtnachricht

```
HIRMG:2:2+0010::Nachricht entgegengenommen'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Beispieldialog	Stand: 02.02.1998	Seite: 45

Segment: Rückmeldungen zu Segmenten

HIRMS:3:2:4+0010::Auftrag entgegengenommen'

Segment: Datensegmente

Segment: Nachrichtenabschluß

HNHBS:4:1+2'

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 46	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Beispieldialog

VIII.5.3 Nachricht „Saldenabfrage“

a) Kundennachricht

Die Kundennachricht wird nur von Benutzer '12345' signiert.

Segment: Nachrichtenkopf

```
HNHBK:1:2+000000000257+201+4711+3'
```

Segment: Signaturkopf

```
HNSHK:2:3+1+654321+1+1+1::2+3234+1:19960701:111144+1:999:1+6:10:16+280:10020030:12345:S:1:1'
```

Segment: Saldenabfrage

```
HKSAL:3:3+1234567:280:10020030+N'
```

Segment: Signaturabschluß

```
HNSHA:4:1+654321+@96@<Signatur>'
```

Segment: Nachrichtenabschluß

```
HNHBS:5:1+3'
```

b) Kreditinstitutsnachricht

Segment: Nachrichtenkopf

```
HNHBK:1:2+000000000213+201+4711+3+4711:3'
```

Segment: Rückmeldungen zur Gesamtnachricht

```
HIRMG:2:2+0010::Nachricht entgegengenommen'
```

Segment: Rückmeldungen zu Segmenten

```
HIRMS:3:2:3+0020::Auftrag ausgeführt'
```

Segment: Datensegmente

```
HISAL:4:3:3+1234567:280:10020030+Giro Spezial+DE  
M+C:1000,:DEM:19960701+D:500,:DEM:19960701+5000,  
:DEM+7138,35:DEM+1476,98:DEM'
```

Segment: Nachrichtenabschluß

```
HNHBS:5:1+3'
```

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Beispieldialog	Stand: 02.02.1998	Seite: 47

VIII.5.4 Nachricht „Dialogbeendigung“

a) Kundennachricht

Segment: Nachrichtenkopf

```
HNHBK:1:2+0000000000475+201+4711+4'
```

Segment: Signaturkopf

```
HNSHK:2:3+1+654321+1+1+1::2+3234+1:19960701:1111  
44+1:999:1+6:10:16+280:10020030:12345:S:1:1'
```

Segment: Dialogende

```
HKEND:3:1+4711'
```

Segment: Signaturabschluß

```
HNSHA:4:1+654321+@96@<Signatur>'
```

Segment: Nachrichtenabschluß

```
HNHBS:5:1+4'
```

b) Kreditinstitutsnachricht

Segment: Nachrichtenkopf

```
HNHBK:1:2+0000000000385+201+4711+4+4711:4'
```

Segment: Rückmeldungen zur Gesamtnachricht

```
HIRMG:2:2+0100::Dialog beendet'
```

Segment: Rückmeldungen zu Segmenten

```
HIRMS:3:2:3+0020::Auftrag ausgeführt'
```

Segment: Datensegmente

Segment: Nachrichtenabschluß

```
HNHBS:4:1+4'
```


Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Transportmedienspezifische Festlegungen	Stand: 02.02.1998	Seite: 49

VIII.6 Transportmedienspezifische Festlegungen

Obwohl HBCI grundsätzlich unabhängig von darunterliegenden Kommunikationsschichten ist, müssen doch bestimmte Festlegungen für die zuliefernden Netze getroffen werden, um HBCI multibankfähig und einheitlich zu definieren.

Hierbei handelt es sich um folgende Aspekte:

- Einschränkung der Kombinationsmöglichkeit von Protokollen, die für die gesicherte Übertragung von HBCI-Datenströmen zugelassen werden.
- Festlegung von verwendeten Parametern.
- Abbilden von HBCI-Dialogabläufen auf die darunterliegenden Strukturen.

Zur Zeit sind die folgenden beiden Transportdienste beschrieben:

- T-Online unter CEPT/EHKP/BtxFIF
- TCP/IP

VIII.6.1 T-Online

T-Online setzt im Rahmen seiner Vorgaben für den Externen Rechnerverbund eine Protokollstruktur voraus, die auf X.25 (Datex-P) aufsetzt und die beiden Anschlußmöglichkeiten EHKP bzw. X.29 erlaubt. Die Alternative X.29 wird hier nicht beschrieben. Für die Übertragung von HBCI-Nachrichten werden, abhängig von der verwendeten Anschlußart, die folgenden Festlegungen getroffen.

Realisierung Bank: alternativ verpflichtend (es muß entweder der T-Online- oder der TCP/IP-Zugang realisiert werden)

Realisierung Kunde: verpflichtend (sofern keine hardwaretechnischen Restriktionen vorliegen)

VIII.6.1.1 ETSI 300 072 („CEPT“)

ETSI 300 072 beschreibt einen Darstellungs- und Datenübertragungsstandard. HBCI-Daten werden im „Transparenten Modus des Leitungsprotokolls“ innerhalb des CEPT-Datenstromes übertragen.

Die in ETSI 300 072 beschriebene Datenflußkontrolle erlaubt auch die Verwendung von Endgeräten, die eine Fehlerkorrektur nach V.42 bzw. MNP4 durch das Modem nicht erlauben.

Dialoginitialisierung, Nachrichtenübertragung und Dialogende werden in folgender Weise im T-Online Dialogprotokoll abgebildet:

a) Dialoginitialisierung

Um zu vermeiden, daß trotz gleichen Aufbaus der T-Online-Übergabeseite für jede Institutsgruppe separate Decodermakros geschaffen werden müssen, werden für die Gestaltung der Übergabeseite folgende Vorgaben getroffen:

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 50	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Transportmedienspezifische Festlegungen

Spalte 6

Impressum

Raum für freie Gestaltung durch das Kreditinstitut

Zeile 10

BLZ: BLZ Länge: 8

HNHBK:1:1+0+1+N`
 HNSHK:2:1+1+654321+1+1+1::2+3234+1:19960701:111144+1:999:1+6
 :10:16+280:10020030:12345:S:1:1`
 HKIDN:3:1+280:10020030+12345+2+1`
 HKVSW:4:1+N+N`
 HKVVB:5:1+1+2+3+1+Homebanking Plus+3.0`
 HNSHA:6:1+654321+<Signatur>`
 HNHS:7:1+1`

Transparenter Transportrahmen Länge: 1024

BTX: Teilnehmerkennung (Systemvariable) Länge: 12 Mitbenutzerzusatz (Systemvariable) Länge: 4

Abbildung 22: Aufbau der T-Online-Übergabeseite

Verbindlich ist hierbei die Position des Feldes „Institut“ in Zeile 10/Spalte 6, sowie der Textstring „BLZ: “ in Zeile 10/Spalte 1.

Weiterhin muß die T-Online-Übergabeseite die folgenden Dialogfelder in der beschriebenen Reihenfolge enthalten (es handelt sich nicht um eine HBCI-Formatbeschreibung):

Name	Format	Länge	Status	Anzahl	Belegung unter HBCI
Institut	num	8	M	1	Identifizierung des Kreditinstituts, z.B. über die BLZ
Transparenter Transportrahmen	bin	1024	M	1	für BtxFIF-Datenblöcke
Teilnehmerkennung	an	12	M	1	Systemvariable: Teilnehmerkennung
Mitbenutzerzusatz	an	4	M	1	Systemvariable: Mitbenutzerzusatz

Institut

Hierüber wird kreditinstitutsseitig das zugehörige Kreditinstitut ermittelt. Es wird die 8-stellige Bankleitzahl eingestellt.

Transparenter Transportrahmen

Der Transportrahmen auf der Übergabeseite muß die Dialoginitialisierungsnachricht aufnehmen können. Die Größe dieser Nachricht hängt von zahlreichen Parametern, wie z.B. dem verwendeten Sicherheitsverfahren ab. Legt man Maximalwerte zugrunde, so ist bei den spezifizierten Verfahren ein Wert von 1024 Byte ausreichend. Dies berücksichtigt auch den benötigten Platz für die BtxFIF-Headerdaten und den CEPT-Aufbaucode.

Der BtxFIF-Parameter „Länge der Daten“ ist für diesen ersten Datenblock auf „1024“ einzustellen.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Transportmedienspezifische Festlegungen	Stand: 02.02.1998	Seite: 51

Teilnehmerkennung

Über T-Online wird die Teilnehmerkennung als Systemvariable zur Verfügung gestellt. Die Teilnehmerkennung muß in jedem Falle als Systemvariable eingestellt werden, da deren Vorhandensein den T-Online Dialogablauf beeinflusst (Absenden persönlicher Daten mit „19“).

Mitbenutzerzusatz

Über T-Online wird der Mitbenutzerzusatz als Systemvariable zur Verfügung gestellt. Auch wenn bei einem Institut die Übertragung des Mitbenutzerzusatzes nicht gewünscht sein sollte, muß dieses Feld auf der Seite editiert sein, da sonst die Größe des Transportrahmens nicht standardisiert werden kann.

b) Übertragungsmodus

Nach Empfang der Dialoginitialisierungsnachricht kann der HBCI-Dialog mit einer transparenten Transportseite zur Aufnahme der BtxFIF-Datenblöcke abgewickelt werden. Dies ist eine CEPT-Datensammelseite ohne Aufbaucode, Maskenfelder und Prompttexte mit nur einem transparenten Dialogfeld der maximalen Größe von 1616 Byte. Diese Größe muß bei kleineren Nachrichten entsprechend angepaßt und mit dem BtxFIF-Parameter „Länge der Daten“ abgeglichen werden.

Die transparenten Dialogfelder für die Übertragung der BtxFIF-Blöcke besitzen grundsätzlich das Attribut „geschützt“. Ausnahme bildet der jeweils letzte Block einer Kreditinstitutsnachricht. Hier muß das Dialogfeld die Eingabe transparenter Daten erlauben (Attribut „ungeschützt“), damit das Kundensystem die nächste HBCI-Nachricht senden kann. Der letzte Block der letzten Kreditinstitutsnachricht ist hingegen als geschütztes Dialogfeld zu senden, da ansonsten das Kundensystem die Transportverbindung nicht trennen kann (siehe unter c) „Dialogende, verursacht durch Kunden“).

T-Online Dialogsteuerungsfunktionen, wie z.B. direkte Seitenwahl, werden nicht verwendet. Der Dialogablauf wird durch HBCI vorgegeben.

Ein HBCI-Dialog muß ohne Unterbrechungen durch Benutzereingaben abgewickelt werden, da für die Übertragung transparenter Daten seitens des T-Online Zugangsrechners eine Zeitüberwachung erfolgt.

c) Dialogende, verursacht durch den Kunden

Das Kundensystem kennzeichnet das Dialogende durch Senden der Dialogendnachricht. Der letzte BtxFIF-Block der zugehörigen Antwortnachricht beendet auch die logische HBCI-Session. Das transparente Dialogfeld zur Übertragung des letzten BtxFIF-Blockes der letzten Kreditinstitutsnachricht erhält das Attribut „geschützt“.

Das Kundensystem muß nun über *0# den Externen Rechner verlassen, um ein logisches Ende der Session herbeizuführen. Anschließend kann nach evtl. Wechsel des Sicherheitsmediums eine neue logische Session durch Absenden einer neuen Dialoginitialisierung aufgebaut werden bzw. die T-Online-Verbindung komplett beendet werden (*9#, Modembefehl ATH, oder ähnliches)

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 52	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Transportmedienspezifische Festlegungen

d) Dialogende, verursacht durch das Kreditinstitut

Das Kreditinstitut sendet synchron eine HBCI-Antwortnachricht mit Bestätigung des Dialogendes im letzten BtxFIF-Block. Es wird keine CEPT-Abschiedsseite ausgegeben.

VIII.6.1.2 EHKP

Die EHKP-Protokolle („Einheitlich Höhere Kommunikations-Protokolle“) der Schicht 4 und 6 sorgen für eine gesicherte Kommunikation zwischen T-Online Netzknoten und Externem Rechner. Hierbei besteht durch EHKP6 die Beschränkung auf eine maximale Dialogfeldlänge von 1616 Byte bei Verwendung eines einzigen Dialogfeldes auf einer Transportseite ohne Aufbaucode, Maskenfelder und Prompttexte. Um diese Begrenzung aufzuheben, wird zusätzlich BtxFIF für die Fragmentierung der HBCI-Nachrichten eingesetzt.

VIII.6.1.3 BtxFIF

BtxFIF („Btx File Interchange Format“) erlaubt die beidseitige Übertragung beliebiger 8-bit kodierter transparenter Datenströme in einem blockorientierten Protokoll. Es werden zwei unterschiedliche Nachrichtenstrukturen verwendet:

♦ **Struktur des 1. Datenblocks**

Vorspann	Länge Header	Länge Daten	Block Header	Datei Header	Daten
----------	--------------	-------------	--------------	--------------	-------

♦ **Struktur der folgenden Datenblöcke**

Vorspann	Länge Header	Länge Daten	Block Header	Daten
----------	--------------	-------------	--------------	-------

♦ **Festlegungen**

Abgesehen von den unten aufgeführten Belegungsregeln gelten die Definitionen der BtxFIF-Beschreibung der Deutschen Telekom, insbesondere die Syntax für den Datenaufbau (Tag-Length-Value).

Aufbauend auf diesen Definitionen werden folgende Festlegungen getroffen:

Länge der Daten

Die Länge der Daten, die in einem Block übertragen werden, muß mit der Größe des transparenten Transportrahmens übereinstimmen, bei maximaler Auslegung sind dies 1616 Byte (vgl. Kapitel VIII.6.1.1.1 und VIII.6.1.1.2).

♦ **Parameter im Block Header**

(Es handelt sich nicht um eine HBCI-Formatbeschreibung)

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Transportmedienspezifische Festlegungen	Stand: 02.02.1998	Seite: 53

Name	Format	Länge	Status	Belegung unter HBCI
Transfer-ID	an	4	M	beliebiger 4-stelliger Wert
Blocknummer	bin	2	M	16-bit Zähler
Anzahl der Blöcke	bin	2	M	16-bit Zähler
Restartcode			K	
Continuecode			K	leer bzw. ETSI 300 072 '#'

♦ Erläuterungen zum Block Header

Das BtxFIF-Feld „Restartcode“ ist nicht zu belegen, da auf Transportebene kein Restart durchgeführt wird. Das BtxFIF-Feld „Block Kontrollsumme“ ist nicht zu belegen, da die Kontrolle über die Unversehrtheit der Daten bei HBCI durch die Hashwertbildung erreicht wird.

Transfer-ID

Hier kann ein beliebiger 4-stelliger alphanumerischer Wert als Referenz für die aktuell zu übertragende Nachricht eingestellt werden. Dieser geht in die Bildung des Dateinamens mit ein (siehe Datei Header).

Blocknummer

Nummer des aktuell zu übertragenden Blocks, stetig lückenlos aufsteigend, beginnend bei 1.

Anzahl der Blöcke

Anzahl der zu übertragenden Blöcke für die gesamte HBCI-Nachricht.

Continuecode

Bei nur einem Übertragungsblock ist das Feld nicht zu belegen, bei mehreren Blöcken ist ETSI 300 072 '#' einzustellen.

♦ Parameter im Datei Header

(Es handelt sich nicht um eine HBCI-Formatbeschreibung)

Name	Format	Länge	Status	Belegung unter HBCI
Dateiname	an	12	M	DOS-kompatibler Name ohne Pfad
Datum/Uhrzeit	an	12	M	JJMMTTThhmmss bzw. 00 ... 00
Dateilänge	bin	..8	M	64-bit Länge der HBCI-Daten
Dateityp	num	1	M	'0' für binäre Daten
Datei Kontrollsumme	bin	4	M	32-bit Frame Check Sequence (FCS)

♦ Erläuterungen zum Datei Header

Die BtxFIF-Felder 'Ziel Name', 'Benutzerfeld' und 'Kompression' dürfen nicht belegt werden.

Dateiname

DOS-kompatibler Datei Name im Format HBCI####.HBC, wobei unter #### die 4-stellige Transfer-ID (siehe Block Header) zu verstehen ist.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 54	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Transportmedienspezifische Festlegungen

Datum/Uhrzeit

Datum und Uhrzeit der Übertragung gemäß o.a. Format. Der Inhalt dieses Zeitstempels wird nicht auf Plausibilität geprüft und ist bei Endgeräten ohne Datumseinrichtung durch die Ziffernfolge 00 ... 00 zu ersetzen.

Dateilänge

Länge der gesamten HBCI-Nachricht gemäß BtxFIF in 64-bit kodiert.

Dateityp

Für die Übertragung von binären Daten ist als Dateityp '0' einzustellen.

Datei Kontrollsumme

Frame Check Sequence (FCS) gemäß CCITT-Empfehlung V.42. Diese Kontrollsumme ist durch BtxFIF zwingend vorgeschrieben.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Transportmedienspezifische Festlegungen	Stand: 02.02.1998	Seite: 55

VIII.6.2 TCP/IP

Realisierung Bank: alternativ verpflichtend (es muß entweder der T-Online- oder der TCP/IP-Zugang realisiert werden)

Realisierung Kunde: verpflichtend (sofern keine hardwaretechnischen Restriktionen vorliegen)

Das „Transport Control Protocol“ (TCP) stellt eine Anwendungsschnittstelle zur Verfügung, auf der Applikationen aufsetzen können, um HBCI-Nachrichten auf gesichertem Weg zwischen Kunde und Kreditinstitut zu übertragen. Da TCP/IP selbst keinen Dialogbezug zwischen den einzelnen HBCI-Nachrichten herstellen kann, muß dies durch ein auf TCP/IP aufsetzendes Dialogprotokoll sichergestellt werden.

Es ist darauf zu achten, daß nur der in RFC793 beschriebene Mindestumfang an Protokollkommandos zum Einsatz kommt, um eine möglichst hohe Kompatibilität zu erreichen.

Als zu verwendende Port Nummer wurde die Adresse 3000 bei der „Internet Assigned Numbers Authority“ (IANA) registriert. Als Schnittstelle zwischen dem TCP/IP-Protokoll als Kommunikationspfad und dem HBCI-Kreditinstitutssystem auf der Anwendungsseite ist ausschließlich die Verwendung von Sockets¹ bzw. einer zu der Socketschnittstelle 100% kompatiblen Netzwerkschnittstelle zulässig. Diese Forderung ist hinsichtlich der bereits zu Anfang des Kapitels geschilderten Rahmenbedingungen bezüglich der Einheitlichkeit und Multibankfähigkeit von HBCI auf der Seite der Kommunikationsschnittstelle des Kunden erforderlich.

Der TCP/IP-Zugang kann verwendet werden, um einen HBCI-Zugang zum Internet oder einen direkten Kreditinstitutszugang zu ermöglichen.

VIII.6.2.1 Internet (WWW)

HBCI ist unabhängig von der verwendeten Komponente aus der Liste der Internet-Anwendungen (z.B. World Wide Web, FTP, Telnet). Zu berücksichtigen ist allerdings die Transparenz des verwendeten Internet-Service, d.h. es muß evtl. eine Filterfunktion eingesetzt werden.

Aufgrund der in HBCI integrierten Sicherheitsmechanismen wird auf die Verwendung von Internet-spezifischen Sicherheitsprotokollen (z.B. SSL) bewußt verzichtet.

VIII.6.2.2 Direktzugang

VIII.6.2.2.1 Protokollanforderungen

Falls ein Kreditinstitut den Direktzugang nutzen möchte, kann es dies mit Hilfe des Protokollstacks TCP/IP und PPP realisieren. Die Konfiguration des Kundenzu-

¹ Die Implementierung der Socketschnittstelle setzt auf dem TCP/IP-Protokollstack auf und bietet eine weitestgehend plattformunabhängige Kommunikationsschnittstelle auf der Basis des TCP/IP-Protokolls. Sockets - als Medium für eine netzwerkübergreifende Prozeßkommunikation - sind ursprünglich ein Medium der Interprozeßkommunikationsschnittstellen des UNIX-Betriebssystems und haben sich als Herstellerstandard in diesem Umfeld etabliert. Entsprechende Portierungen der Socketschnittstelle liegen heute auf allen gängigen Betriebssystemplattformen (Windows 3.1/95/ NT, OS/2, Macintosh usw.) vor.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 56	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Transportmedienspezifische Festlegungen

gangs kann jedoch dabei aufgrund des Umfangs der erforderlichen Parameter nicht über HBCI erfolgen. Es sind daher bilaterale Absprachen zwischen Kunde und Kreditinstitut erforderlich. Zu einem späteren Zeitpunkt, wenn sich eine PPP-Variante als Standard herausgebildet hat, läßt sich der Direktzugang evtl. konkreter beschreiben.

VIII.6.2.2.2 Sicherheitsanforderungen

Verbindliche Sicherheitsanforderungen werden im nächsten Release der Schnittstellenspezifikation nachgereicht.

VIII.6.3 Sonstige Kommunikationsdienste

Wird die Kommunikation über einen bisher nicht erfaßten Kommunikationsdienst angestrebt, so sind zur Sicherstellung der Multibankfähigkeit vorab alle weiteren Spezifikationen durch die Kreditinstitute einheitlich festzulegen.

Wie bei den vorgenannten Kommunikationsdiensten muß auch bei den neu zu definierenden Kommunikationsbeziehungen sichergestellt sein, daß diese einen Dialogbezug zwischen den einzelnen HBCI-Nachrichten herstellen können.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Abruf von Kommunikationszugangsdaten	Stand: 02.02.1998	Seite: 57

VIII.7 Abruf von Kommunikationszugangsdaten

Für den Aufbau einer Verbindung zu einem Kreditinstitut sind bestimmte netz- und dienstspezifische Zugangsdaten erforderlich. Diese Daten müssen dem Kundensystem bereits vorliegen, bevor es die Verbindung aufbauen kann. Mit Hilfe dieses Auftrags wird dem Kunden die Möglichkeit gegeben, sich einen Zugangsdatenbestand anzulegen bzw. diesen zu aktualisieren.

Realisierung Bank: optional

Realisierung Kunde: optional

a) Kundenauftrag

◆ Beschreibung

Eine Dialoginitialisierung als anonymer Benutzer ist erforderlich. Anschließend an die Dialoginitialisierung darf nur eine Nachricht mit dem Segment „Kommunikationszugang anfordern“ folgen. Nach Erhalt der Antwortnachricht wird der Dialog in jedem Fall beendet. Die Anforderung der Kommunikationszugänge darf nicht während eines „regulären“ HBCI-Dialogs erfolgen. Der Auftrag wird in diesem Fall abgelehnt.

◆ Format

Name: Kommunikationszugang

Typ: Nachricht

Sender: Kunde

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	
2	Kommunikationszugang anfordern	SEG	HKKOM	M	1	
3	Nachrichtenabschluß	SEG	HNHBS	M	1	

Name: Kommunikationszugang anfordern

Typ: Segment

Segmentart: Geschäftsvorfall

Kennung: HKKOM

Bezugssegment: -

Segmentversion: 2

Sender: Kunde

Nr.	Name	Typ	For- mat	Län- ge	Sta- tus	An- zahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Von BLZ	DE	num	8	K	1	
3	Bis BLZ	DE	num	8	K	1	
4	Maximale Anzahl Einträge	DE	num	..4	K	1	>0
5	Aufsetzpunkt	DE	an	..35	K	1	

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 58	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Abruf von Kommunikationszugangsdaten

♦ Erläuterungen

Nr. 2,3: Von BLZ, Bis BLZ

In die DE „Von BLZ“ und „Bis BLZ“ können Bankleitzahlen eingestellt werden, um den Bereich der gewünschten Kommunikationszugänge einzugrenzen. Wird kein BLZ-Bereich eingestellt, so werden alle verfügbaren Kommunikationszugänge rückgemeldet.

Nr. 4: Maximale Anzahl Einträge

Es kann die Anzahl der rückzumeldenden Kommunikationszugänge begrenzt werden (s. Kap. II.7.3).

Nr. 5: Aufsetzpunkt

Belegung nur zulässig, wenn vom Kreditinstitut ein Aufsetzpunkt rückgemeldet wurde (s. Kap. II.7.3).

♦ Beispiel

Alle Kommunikationszugänge:

HKKOM: 2 : 2 '

Kommunikationszugänge für BLZ 100 200 30:

HKKOM: 2 : 2+10020030+10020030 '

b) Kreditinstitutsrückmeldung

♦ Beschreibung

Für jedes der vom Kunden angeforderten Kreditinstitute wird ein Segment des Formats „Kommunikationszugang rückmelden“ in die Kreditinstitutsnachricht eingestellt.

Die Einstellung von Zeiten, während derer das Kreditinstitut erreichbar ist, erfolgt nicht, da diese häufigeren Änderungen unterworfen sein können. Grundsätzlich ist eine 24-stündige Erreichbarkeit anzustreben.

♦ Format

Name: Antwort auf Kommunikationszugang
Typ: Nachricht
Sender: Kreditinstitut

Nr.	Name	Typ	Ken- nung	Sta- tus	An- zahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	
2	Rückmeldungen zur Gesamtnachricht	SEG	HIRMG	M	1	
3	Rückmeldungen zu Segmenten	SEG	HIRMS	K	0..1	
4	Kommunikationszugang rückmelden	SEG	HIKOM	K	0..n	
5	Nachrichtenabschluß	SEG	HNHBS	M	1	

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Abruf von Kommunikationszugangsdaten	Stand: 02.02.1998	Seite: 59

Name: Kommunikationszugang rückmelden
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIKOM
 Bezugssegment: HKKOM
 Segmentversion: 2
 Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kreditinstitutskennung	DEG	kik	#	M	1	
3	Standardsprache	DE	num	..3	M	1	1,2,3
4	Kommunikationsparameter	DEG			M	1..9	

◆ Erläuterungen

Nr. 3: Standardsprache

Es ist ein Sprachkennzeichen gemäß Kap. III.3.1.3 einzustellen, welches Standardsprache und -zeichensatz des Kreditinstituts festlegt. Dieses Kennzeichen bestimmt, mit welchem Zeichensatz die Dialoginitialisierungsnachricht des Kunden gebildet werden muß. Nach dieser Nachricht verliert die Standardsprache ihre Gültigkeit, da der Kunde in der Dialoginitialisierung die Dialogsprache wählt, welche evtl. von der Standardsprache abweicht.

Nr. 4: Kommunikationsparameter

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Kommunikationsdienst	GD	num	..2	M	1	1,2
2	Kommunikationsadresse	GD	an	..512	M	1	
3	Kommunikationsadressenzusatz	GD	an	..512	K	1	
4	Filterfunktion	GD	an	3	K	1	MIM, UUE
5	Version der Filterfunktion	GD	num	..3	K	1	

Nr. 1: Kommunikationsdienst

Unterstütztes Kommunikationsverfahren (Protokollstack), auf daß sich Nachstehendes bezieht (s. Kap. „Transportmedienspezifische Festlegungen“).

Zur Zeit unterstützte Kommunikationsverfahren:

Code	Zugang	Protokollstack
1	T-Online	ETSI 300 072 (CEPT), EHKP, BtxFIF
2	TCP/IP	SLIP/PPP

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 60	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Abruf von Kommunikationszugangsdaten

Nr. 2: Kommunikationsadresse

Abhängig vom Kommunikationsverfahren sind folgende Informationen einzustellen:

Zugang	Adresse	Anmerkungen
T-Online	Gateway-Seite	als numerischer Wert (ohne die Steuerzeichen * und #) einzustellen.
TCP/IP	IP-Adresse	

Nr. 3: Kommunikationsadressenzusatz

Abhängig vom Kommunikationsverfahren sind folgende Informationen einzustellen:

Zugang	Adressenzusatz	Anmerkungen
T-Online	Regionalbereich	Für ein bundesweites Angebot ist '00' einzustellen'
TCP/IP	nicht belegt	

Nr. 4: Filterfunktion

Falls das Übertragungsverfahren eine Umwandlung der Nachricht in eine 7 Bit-Zeichendarstellung erfordert (z.B. Internet), so ist hier das anzuwendende Filterverfahren anzugeben. Die Nachricht ist stets komplett zu filtern, auch wenn eine Filterung nicht notwendig wäre, da bspw. keine binären Daten enthalten sind.

Ein Kreditinstitut darf jeweils nur eine Filterfunktion unterstützen.

Zugelassene Filterfunktionen:

Code	Bedeutung
MIM	MIME Base 64
UUE	Uuencode/Uudecode

Nr. 5: Version der Filterfunktion

Dieses DE darf nur belegt werden, falls eine Filterfunktion angegeben wurde.

◆ Beispiel

```
HIKOM:3:2:2+280:10020030+1+1:12345678:00+2:123.4
56.789.01::UUE:1 '
HIKOM:4:2:2+280:20030040+1+1:54321:00 '
HIKOM:5:2:2+280:30040050+2+1:12345:22 '
```

◆ Ausgewählte Beispiele für Rückmeldungs-codes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
3010	Es liegen keine Einträge vor
3040	Auftrag nur teilweise ausgeführt

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Abruf von Kommunikationszugangsdaten	Stand: 02.02.1998	Seite: 61

9210	Bereichende darf nicht vor Bereichanfang liegen
------	---

c) Bankparameterdaten

◆ Format

Name: Kommunikationszugang Parameter
 Typ: Segment
 Segmentart: Geschäftsvorfall
 Kennung: HIKOMS
 Bezugssegment: HKVVB
 Segmentversion: 2
 Sender: Kreditinstitut
 Format: Geschäftsvorfallparameter

◆ Erläuterungen

Nr. 4: Parameter

Die DEG wird nicht belegt.

◆ Beispiel

HIKOMS:11:2:5+1+2 '



Das Anfordern der Kommunikationszugänge ist insbesondere für den Erstzugang erforderlich. Weiterhin werden Zugangsdaten für den anonymen Zugang (Gastzugang) benötigt. Kommunikationszugänge sind keinen ständigen Änderungen unterworfen und müssen daher nur in großen Zeitabständen aktualisiert werden. Eine Aktualisierung kann auch automatisch erfolgen, sofern ein Verbindungsaufbau aufgrund veralteter Zugangsdaten fehlschlägt.

Die Zugangsdaten sollten für spätere Zugänge im Kundenprodukt gespeichert werden. Aus Effizienzgründen kann diese Zugangsdatenbank im Kundenprodukt mit einer lokalen Bankleitzahlendatei verknüpft werden.

Es ist zu berücksichtigen, daß die Kommunikationsadresse, unter der die Zugangsdaten abgerufen werden, im Regelfall nicht identisch ist mit der Adresse des Kreditinstituts, zu dem der Zugang aufgebaut werden soll, so daß u.U. nach dem Aktualisieren der Zugangsdaten die physikalische Verbindung erst beendet und dann mit den neuen Zugangsdaten erneut aufgebaut werden muß.

Jeder Verband pflegt die Zugangsdaten seiner angeschlossenen Institute und bietet sie an zentraler Stelle zum Abruf an. Die jeweilige Abrufadresse kann bei den in der Einleitung dieses Dokumentes genannten Ansprechpartnern erfragt werden.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Chipapplikation für DDV	Stand: 02.02.1998	Seite: 63

VIII.8 Chipapplikation für DDV

Im folgenden wird für das in Kap. VI beschriebene DDV-Verfahren eine entsprechende Chipanwendung namens „Banking“ spezifiziert. Voraussetzung ist neben den nachfolgend beschriebenen Datenelementen zusätzlich das Vorhandensein des Datenelements EF_ID sowie des Kryptoalgorithmus Triple-DES, wie sie in der „Schnittstellenspezifikation für die ec-Karte mit Chip“ vom ZKA festgelegt wurden. Die Spezifikation bezieht sich allein auf die für HBCI erforderlichen Datenelemente.

Die Anwendung „Banking“ kann auf einer dedizierten Chipkarte („HBCI-Karte“) oder auf beliebigen multifunktionalen Chipkarten implementiert werden, sofern sie das Betriebssystem der ec-Karte mit Chip einsetzen. Für die HBCI-Anwendung ist kein ausführbarer Code über die Spezifikationen in ISO 7816-4 bzw. der ec-Karte mit Chip hinaus erforderlich.

Die folgende Grafik gibt einen Überblick über die Datenelemente (EFs) der Applikation „Banking“.

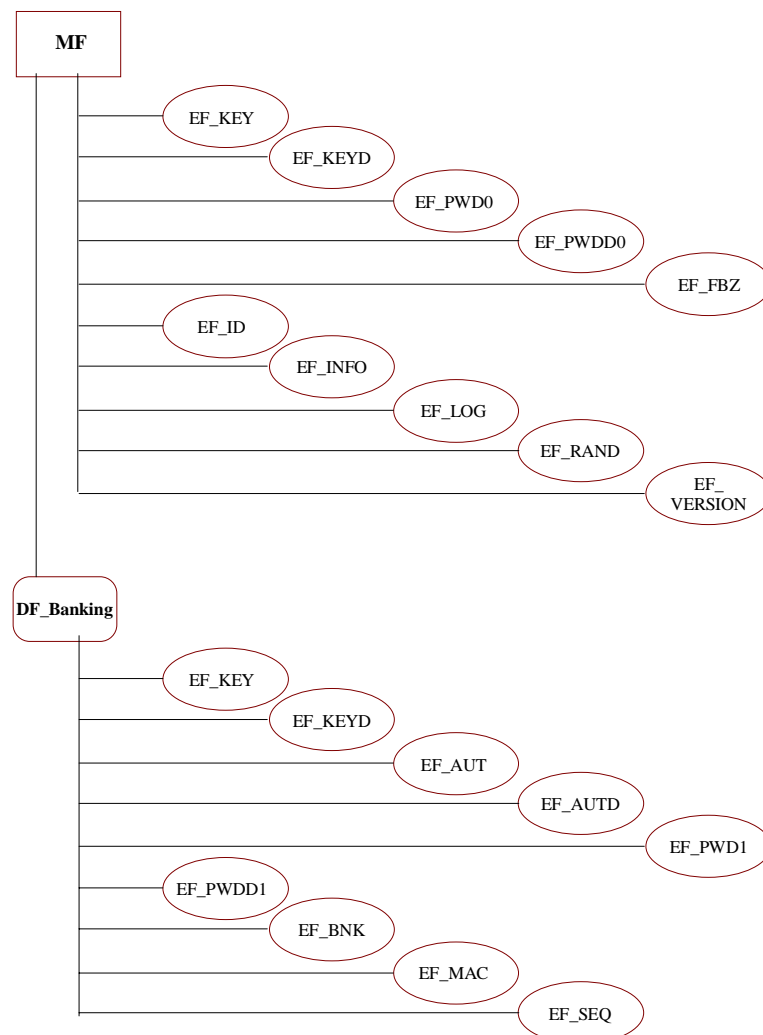


Abb. 23: Datenelemente der Applikation „Banking“

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 64	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Chipapplikation für DDV

VIII.8.1 DF_Banking

◆ Beschreibung

Der Applikation DF_Banking sind 4 Datenfelder als AEFs zugeordnet, die für das HBCI-Endgerät über Lese- und Schreibzugriff zugänglich sind:

SFI '19'	EF_ID im MF
SFI '1A'	EF_BNK im DF_Banking
SFI '1B'	EF_MAC im DF_Banking
SFI '1C'	EF_SEQ im DF_Banking

Wenn das DF_Banking mittels SELECT FILE selektiert wird und eine entsprechende Option im Parameter P2 des Kommandos gesetzt ist, werden die folgenden FMD mit den Pfaden der AEFs ausgegeben (hierbei wird vorausgesetzt, daß sich das DF_Banking direkt im MF befindet).

◆ Format

Tag	Länge	Wert	Erläuterung
'64'	'1A'		Tag und Länge für FMD
'85'	'03'	'19 00 03'	Pfad für das AEF mit SFI '19' (EF_ID im MF)
'85'	'05'	'1A A6 00 03 01'	Pfad für das AEF mit SFI '1A' (EF_BNK im DF_Banking)
'85'	'05'	'1B A6 00 03 02'	Pfad für das AEF mit SFI '1B' (EF_MAC im DF_Banking)
'85'	'05'	'1C A6 00 03 03'	Pfad für das AEF mit SFI '1C' (EF_SEQ im DF_Banking)

Ebenfalls über den Parameter P2 kann mit dem SELECT FILE der folgende FCI mit den ACs der AEFs im zusammengesetzten Datenobjekt mit Tag 'A5' ausgegeben werden.

Tag	Länge	Wert	Erläuterungen
'6F'	'40'		Tag und Länge für FCI
'81'	'02'	'xxxx'	freier Speicherplatz in der ec-Karte
'82'	'01'	'38'	Datei-Deskriptor für DF
'83'	'02'	'A600'	Datei-ID der Applikation 'Banking'
'84'	'09'	'D27600002548420100'	DF-Name (AID) des DF_Banking
'86'	'02'	'0040'	AC für DF_Banking
'A5'	'24'		Tag und Länge der ACs der AEFs
'86'	'07'	'19 0040 0000 00F0'	SFI und ACs des EF_ID
'86'	'07'	'1A 0040 0000 0031'	SFI und ACs des EF_BNK
'86'	'07'	'1B 0040 3150 0031'	SFI und ACs des EF_MAC
'86'	'07'	'1C 0040 0000 0031'	SFI und ACs des EF_SEQ

◆ Erläuterungen

Tag '83':

Die Datei-ID der Applikation 'Banking' lautet A600.

Tag '84':

Application Identifier (AID) für Homebanking mit Chipkarte

Tag '86':

Kommandogruppe ADMIN: AC '0040' (PRO_G mit Schlüsselnummer '00')

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Chipapplikation für DDV	Stand: 02.02.1998	Seite: 65

VIII.8.2 EFs im DF_Banking

VIII.8.2.1 EF_KEY

◆ Beschreibung

In diesem EF wird der kundenindividuelle Signierschlüssel abgelegt.

◆ Format

File Control Parameter (FCP):

Tag	Länge	Wert	Erläuterung
'62'	'15'		Tag und Länge für FCP
'81'	'02'	'00 11'	allokierter Speicherplatz in Byte
'82'	'03'	'02 41 11'	Datei-Deskriptor für lineares EF
'83'	'02'	'00 10'	Datei-ID des EF_KEY
'86'	'06'	'0060 00F0 0060'	ACs für das EF_KEY

◆ Erläuterungen

Tag '81':

Das EF_KEY enthält maximal einen Record in der Länge 17 Byte, so daß 17 Byte benötigt werden.

Tag '82':

Die Recordlänge beträgt 17 Byte (X'11').

Tag '83':

Die Datei-ID muß '00 10' lauten bei einem EF_KEY.

Tag '86':

APPEND RECORD: AC '00 60' (ENC_G mit Schlüsselnummer '00')

READ RECORD: AC '00 F0' (NEV)

UPDATE RECORD: AC '00 60' (ENC_G mit Schlüsselnummer '00')

Daten:

Das EF_KEY des DF_Banking enthält einen Record. Der Record enthält die logische Schlüsselnummer mit dem Signierschlüssel.

Logische Schlüsselnr.	Schlüssel
'00'	16 Byte lange K_{DSG}

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 66	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Chipapplikation für DDV

VIII.8.2.2 EF_KEYD

◆ Beschreibung

Dieses EF dient der Beschreibung der Eigenschaften des Signierschlüssels.

◆ Format

File Control Parameter (FCP):

Tag	Länge	Wert	Erläuterung
'62'	'15'		Tag und Länge für FCP
'81'	'02'	'00 05'	allokierter Speicherplatz in Byte
'82'	'03'	'02 41 05'	Datei-Deskriptor für lineares EF
'83'	'02'	'00 13'	Datei-ID des EF_KEYD
'86'	'06'	'0040 0000 0040'	ACs für das EF_KEYD

◆ Erläuterungen

Tag '81':

Das EF_KEYD enthält maximal einen Record in der Länge 5 Byte, so daß 5 Byte benötigt werden.

Tag '82':

Die Recordlänge beträgt 5 Byte.

Tag '83':

Die Datei-ID muß '00 13' lauten bei einem EF_KEYD.

Tag '86':

APPEND RECORD: AC '00 40' (PRO_G mit Schlüsselnummer '00')

READ RECORD: AC '00 00' (ALW)

UPDATE RECORD: AC '00 40' (PRO_G mit Schlüsselnummer '00')

Daten:

Für jeden im EF_KEY gespeicherten Schlüssel muß ein Record, der die jeweilige logische Schlüsselnummer und weitere Parameter enthält, im EF_KEYD enthalten sein.

Log. Schlüsselnr.	Schlüssel- länge	Algorithmus- ID	FBZ	Schlüsselversion
'00'	'10'	'07'	'FF'	'00'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Chipapplikation für DDV	Stand: 02.02.1998	Seite: 67

VIII.8.2.3 EF_AUT

◆ Beschreibung

In diesem EF wird der kundenindividuelle Chiffrierschlüssel abgelegt.

◆ Format

File Control Parameter (FCP):

Tag	Länge	Wert	Erläuterung
'62'	'15'		Tag und Länge für FCP
'81'	'02'	'00 11'	allokierter Speicherplatz in Byte
'82'	'03'	'02 41 11'	Datei-Deskriptor für lineares EF
'83'	'02'	'00 11'	Datei-ID des EF_AUT
'86'	'06'	'0060 00F0 0060'	ACs für das EF_AUT

◆ Erläuterungen

Tag '81':

Das EF_AUT enthält maximal einen Record in der Länge 17 Byte, so daß 17 Byte benötigt werden.

Tag '82':

Die Recordlänge beträgt 17 Byte (X'11').

Tag '83':

Die Datei-ID muß '00 11' lauten bei einem EF_AUT.

Tag '86':

APPEND RECORD: AC '00 60' (ENC_G mit Schlüsselnummer '00')

READ RECORD: AC '00 F0' (NEV)

UPDATE RECORD: AC '00 60' (ENC_G mit Schlüsselnummer '00')

Daten:

Das EF_AUT der DF_Banking enthält einen Record. Der Record enthält die logische Schlüsselnummer mit dem Schlüssel.

Logische Schlüsselnr.	Schlüssel
'00'	16 Byte lange K _{ENC}

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 68	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Chipapplikation für DDV

VIII.8.2.4 EF_AUTD

◆ Beschreibung

Dieses EF dient der Beschreibung der Eigenschaften des Chiffrierschlüssels.

◆ Format

File Control Parameter (FCP):

Tag	Länge	Wert	Erläuterung
'62'	'15'		Tag und Länge für FCP
'81'	'02'	'00 04'	allokierter Speicherplatz in Byte
'82'	'03'	'02 41 04'	Datei-Deskriptor für lineares EF
'83'	'02'	'00 14'	Datei-ID des EF_AUTD
'86'	'06'	'0040 0000 0040'	ACs für das EF_AUTD

◆ Erläuterungen

Tag '81':

Das EF_AUTD enthält maximal einen Record in der Länge 4 Byte, so daß 4 Byte benötigt werden.

Tag '82':

Die Recordlänge beträgt 4 Byte.

Tag '83':

Die Datei-ID muß '00 14' lauten bei einem EF_AUTD.

Tag '86':

APPEND RECORD: AC '00 40' (PRO_G mit Schlüsselnummer '00')

READ RECORD: AC '00 00' (ALW)

UPDATE RECORD: AC '00 40' (PRO_G mit Schlüsselnummer '00')

Daten:

Für jeden im EF_AUT gespeicherten Schlüssel muß ein Record, der die jeweilige logische Schlüsselnummer und weitere Parameter enthält, im EF_AUTD enthalten sein.

Log. Schlüsselnr.	Schlüssellänge	Algorithmus-ID	Schlüsselversion
'00'	'10'	'07'	'00'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Chipapplikation für DDV	Stand: 02.02.1998	Seite: 69

VIII.8.2.5 EF_PWD1

◆ Beschreibung

In diesem EF wird die anwendungsspezifische Banking-PIN abgelegt.

◆ Format

File Control Parameter (FCP):

Tag	Länge	Wert	Erläuterung
'62'	'17'		Tag und Länge für FCP
'81'	'02'	'00 08'	allokierter Speicherplatz in Byte
'82'	'03'	'02 41 08'	Datei-Deskriptor für lineares EF
'83'	'02'	'00 22'	Datei-ID des EF_PWD1
'86'	'08'	'0060 00F0 0060 00 00'	ACs für das EF_PWD1

◆ Erläuterungen

Tag '81':

Das EF_PWD1 enthält maximal einen Record in der Länge 8 Byte, so daß 8 Byte benötigt werden.

Tag '82':

Die Recordlänge beträgt 8 Byte.

Tag '83':

Die Datei-ID muß '00 22' lauten bei einem EF_PWD1.

Tag '86':

APPEND RECORD: AC '00 60' (ENC_G mit Schlüsselnummer '00')

READ RECORD: AC '00 F0' (NEV)

UPDATE RECORD: AC '00 60' (ENC_G mit Schlüsselnummer '00')

VERIFY AC '00 00' (ALW)

Daten:

Die Banking-PIN ist im 'Format 2 PIN Block' im Record '01' des EF_PWD1 abgelegt. Der Format 2 PIN Block wird gemäß Anhang A von ISO 10202-6 (ISO 13) aus der PIN gebildet. Sie hat eine Mindestlänge von 5 Ziffern und darf maximal 12 Ziffern lang sein. Die 8 Byte des Records sind wie folgt belegt:

C	L	P	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F
---	---	---	---	---	---	---	-----	-----	-----	-----	-----	-----	-----	---	---

Jedes Feld repräsentiert ein Halbbyte:

C:	Kontrollfeld, binär kodiert	hat immer den Wert '2'
L:	PIN-Länge, binär kodiert	mögliche Werte von '5' bis 'C'
P:	PIN-Ziffer, BCD-kodiert	
F:	Filler, Binär kodiert	hat immer der Wert 'F'
P/F:	PIN/Filler	abhängig von der PIN-Länge

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 70	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Chipapplikation für DDV

VIII.8.2.6 EF_PWDD1

◆ Beschreibung

Dieses EF dient der Beschreibung der Eigenschaften der Banking-PIN.

◆ Format

File Control Parameter (FCP):

Tag	Länge	Wert	Erläuterung
'62'	'15'		Tag und Länge für FCP
'81'	'02'	'00 05'	allokierter Speicherplatz in Byte
'82'	'03'	'02 41 05'	Datei-Deskriptor für lineares EF
'83'	'02'	'00 25'	Datei-ID des EF_PWDD1
'86'	'06'	'0040 0000 0040'	ACs für das EF_PWDD1

◆ Erläuterungen

Tag '81':

Das EF_PWDD1 enthält maximal einen Record in der Länge 5 Byte, so daß 5 Byte benötigt werden.

Tag '82':

Die Recordlänge beträgt 5 Byte.

Tag '83':

Die Datei-ID muß '00 25' lauten bei einem EF_PWDD1.

Tag '86':

APPEND RECORD: AC '00 40' (PRO_G mit Schlüsselnummer '00')

READ RECORD: AC '00 00' (ALW)

UPDATE RECORD: AC '00 40' (PRO_G mit Schlüsselnummer '00')

Daten:

Im 5 Byte langen Record des EF_PWDD1 werden Zusatzinformationen zur Banking-PIN festgehalten:

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5
'01'	'21'	'05'	'03'	'03'

Byte 1: Art der Karteninhaber-Authentikation. Zur Zeit ist nur die Paßwort-Verifikation möglich, die durch den Wert '01' kodiert ist.

Byte 2: Die PIN ist im Format 'Format 2 PIN Block' in BCD gespeichert.

Byte 3: Die PIN muß mindestens 5 Ziffern lang sein.

Byte 4: Initialisierungswert des PIN Fehlbedienungs Zählers in Byte 5.

Byte 5: PIN Fehlbedienungs Zähler.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Chipapplikation für DDV	Stand: 02.02.1998	Seite: 71

VIII.8.2.7 EF_BNK

◆ Beschreibung

Bei dem EF_BNK handelt es sich um ein lineares EF mit 5 Records in denen Bankverbindungen abgelegt sind. Die Bankverbindung kann über T-Online, Internet oder weitere zukünftige Onlinedienste hergestellt werden.

Der Record setzt sich aus einer Bankkurzbezeichnung, der Bankleitzahl, dem Kommunikationsdienst, der Adresse und dem Adresszusatz für den Kommunikationszugang, dem Länderkennzeichen und der Benutzerkennung zusammen.

◆ Format

File Control Parameter (FCP):

Tag	Länge	Wert	Erläuterung
'62'	'15'		Tag und Länge für FCP
'81'	'02'	'01 B8'	allokierter Speicherplatz in Byte
'82'	'03'	'02 41 58'	Datei-Deskriptor für lineares EF
'83'	'02'	'03 01'	Datei-ID des EF_BNK
'86'	'06'	'0040 0000 0031'	ACs für das EF_BNK

◆ Erläuterungen

Tag '81':

Das EF_BNK enthält maximal 5 Records in der Länge 88 Byte, so daß 440 Byte benötigt werden.

Tag '82':

Die Recordlänge beträgt 88 Byte (X'58').

Tag '83':

Als Datei-ID wurde '03 01' für das EF_BNK festgelegt.

Tag '86':

APPEND RECORD: AC '00 40' (PRO_G mit Schlüsselnummer '00')

READ RECORD: AC '00 00' (ALW)

UPDATE RECORD: AC '00 31' (PWD_D)

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 72	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Chipapplikation für DDV

Daten:

Das EF_BNK enthält 5 Records mit folgendem Satzaufbau:

Byte	Länge	Wert	Erläuterung	Referenz
1-20	20	'aa .. aa'	Kurzbezeichner des Kreditinstituts	
21-24	4	'nn nn nn nn'	Bankleitzahl des kontoführenden Instituts	s. II.5.3.2 Nr. 2
25-25	1	'n'	Kommunikationsdienst	s. VIII.7 b) Nr. 1
26-53	28	'aa .. aa'	Kommunikationsadresse	s. VIII.7 b) Nr. 2
54-55	2	'aa aa'	Kommunikationsadressenzusatz	s. VIII.7 b) Nr. 3
56-58	3	'aa aa aa'	Länderkennzeichen des kontoführenden Instituts	s. II.5.3.2 Nr. 1
59-88	30	'aa .. aa'	Benutzerkennung	s. VI.5.1.1 Nr. 2

Alphanumerische Feldinhalte ('a') werden grundsätzlich ASCII-kodiert, linksbündig eingestellt und mit Leerzeichen (X'20') auf die vorgegebene Länge aufgefüllt.

Numerische Feldinhalte ('n') werden grundsätzlich BCD-kodiert.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Chipapplikation für DDV	Stand: 02.02.1998	Seite: 73

VIII.8.2.8 EF_MAC

◆ Beschreibung

Das EF_MAC wird für die MAC-Bildung über den Hashwert einer Nachricht benötigt.

Es besteht aus einem 12 Byte langem Record deren ACs so gesetzt werden müssen, daß beim Lesen des Records der MAC produziert wird.

◆ Format

File Control Parameter (FCP):

Tag	Länge	Wert	Erläuterung
'62'	'15'		Tag und Länge für FCP
'81'	'02'	'00 0C'	allokierter Speicherplatz in Byte
'82'	'03'	'02 41 0C'	Datei-Deskriptor für lineares EF
'83'	'02'	'03 02'	Datei-ID des EF_MAC
'86'	'06'	'0040 3150 0031'	ACs für das EF_MAC

◆ Erläuterungen

Tag '81':

Das EF_MAC enthält maximal einen Record in der Länge 12 Byte, so daß 12 Byte benötigt werden.

Tag '82':

Die Recordlänge beträgt 12 Byte (X'0C').

Tag '83':

Als Datei-ID wurde '03 02' für das EF_MAC festgelegt.

Tag '86':

APPEND RECORD: AC '00 40' (PRO_G mit Schlüsselnummer '00')

READ RECORD: AC '31 50' (PWD_D und PRO_D mit Schlüsselnummer '00')

UPDATE RECORD: AC '00 31' (PWD_D)

Daten:

Das EF_MAC besitzt einen 12 Byte langen Record der durch UPDATE RECORD modifiziert wird.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 74	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Chipapplikation für DDV

VIII.8.2.9 EF_SEQ

◆ Beschreibung

Bei dem EF_SEQ handelt es sich um ein lineares Datenfile, dessen Record ein 2 Byte langes binär definiertes Element enthält.

Dieser binäre aufsteigende Zähler fließt als Sicherheitsreferenznummer (Signatur-ID) zur Absicherung der Daten gegen Doppeleinreichung ein (s. Kap. VI.5.2.1).

Der Startwert des Zählers ist 1. Ein Rücksetzen bei Überlauf findet nicht statt.

◆ Format

File Control Parameter (FCP):

Tag	Länge	Wert	Erläuterung
'62'	'15'		Tag und Länge für FCP
'81'	'02'	'00 02'	allokierter Speicherplatz in Byte
'82'	'03'	'02 41 02'	Datei-Deskriptor für lineares EF
'83'	'02'	'03 03'	Datei-ID des EF_SEQ
'86'	'06'	'0040 0000 0031'	ACs für das EF_SEQ

◆ Erläuterungen

Tag '81':

Das EF_SEQ enthält maximal einen Record in der Länge 2 Byte, so daß 2 Byte benötigt werden.

Tag '82':

Die Recordlänge beträgt 2 Byte.

Tag '83':

Als Datei-ID wurde '03 03' für das EF_SEQ festgelegt.

Tag '86':

APPEND RECORD: AC '00 40' (PRO_G mit Schlüsselnummer '00')

READ RECORD: AC '00 00' (ALW)

UPDATE RECORD: AC '00 31' (PWD_D)

Daten:

Das EF_SEQ besitzt einen 2 Byte langen Record der durch UPDATE RECORD modifiziert wird.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Chipapplikation für DDV	Stand: 02.02.1998	Seite: 75

VIII.8.3 Platzbedarf der Applikation im Chip

Die Platzbedarfsberechnung ist sehr stark von der Stärke der ROM-Maske abhängig. Der notwendige Platz für die EF-Verwaltung z.B. Recordnummern- bzw. Adressverwaltung steht im direkten Zusammenhang mit der Verwaltung des E²-PROM. Diese Verwaltung ist Bestandteil der ROM-Maske. Der tatsächliche exakte Platzbedarf kann nur von den ROM-Maskenentwicklern ermittelt werden. Er ist von Chip zu Chip und ROM-Maske zu ROM-Maske unterschiedlich.

Die nachfolgende Tabelle enthält daher nur die Nettodatengröße der "Banking"-Applikation.

Dateiname	Headergröße	Datengröße
DF_Banking	28	26
EF_KEY	23	17
EF_KEYD	23	5
EF_AUT	23	17
EF_AUTD	23	4
EF_PWD1	25	8
EF_PWDD1	23	5
EF_BNK	23	440
EF_MAC	23	12
EF_SEQ	23	2
	237	536

Größenangaben in Byte

Demnach hat die Applikation "Banking" einen Mindestplatzbedarf von **773 Byte**.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 76	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Chipapplikation für DDV

VIII.8.4 Chipkarten- bzw. Endgeräteabläufe

Nachfolgend werden die Anwendungsabläufe aus Endgerätesicht spezifiziert. Hierbei werden ausschließlich die chipkartenbezogenen Aspekte berücksichtigt. Da die Chipkarte hauptsächlich für die Absicherung von HBCI-Nachrichten eingesetzt wird, sind dies überwiegend sicherheitsrelevante Anwendungsabläufe. Anwendungsbezogene Details wie z.B. Inhalte von HBCI-Aufträgen sind nicht Bestandteil dieser Spezifikation.

Bei den nachfolgenden Abläufen können theoretisch für unterschiedliche Teilabläufe auch unterschiedliche Personen, denen jeweils eine andere Chipkarte zugeordnet ist, zuständig sein. Es wird von dem theoretischen Fall ausgegangen, daß die Teilabläufe des Erzeugens, Signierens (ggf. mehrfach), Verschlüsseln und Sendens von HBCI-Nachrichten von jeweils unterschiedlichen Personen durchgeführt werden können. Konkret bedeutet dies, daß ein Wechsel des Verantwortungsbereichs für einen Teilablauf auch mit einem Wechsel der Chipkarte und erneutem Startdialog (d.h. Reset der Chipkarte, Anwendung selektieren, PIN-Prüfung etc.) verbunden ist. Falls mehrere Teilabläufe von einer Person hintereinander durchgeführt werden, ist dies nicht erforderlich.

Für die Aufbereitung von HBCI-Aufträgen werden z.B. Bankverbindungsdaten benötigt. In den folgenden Abläufen wird davon ausgegangen, daß diese Daten in der Chipkarte gespeichert sind und vom Endgeräteprogramm ausgelesen werden. Dies hat eindeutig Vorteile zugunsten der Mobilität bei gleichzeitig hohem Komfort von HBCI-Anwendungen, z.B. bei Smartphone-Anwendungen. Aber auch die Verwaltung solcher Daten z.B. in einem PC-Programm (z.B. Cash Management Programme) ist denkbar. Zusätzlich kann mehr Flexibilität durch die Möglichkeit zum Editieren solcher Daten erzielt werden.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Chipapplikation für DDV	Stand: 02.02.1998	Seite: 77

VIII.8.4.1 Startdialog

MFC		Endgerät/Gateway		Kreditinstitut	
		<---	A1 Anzeige: 'Bitte Karte einstecken'		
R2	ATR der MFC	--->	C2 Reset MFC		
		<---	C3 SELECT FILE DF_Banking		
R3	AC's, DF-Header	--->	A4 PIN-Eingabe anfordern, PIN formatieren		
		<---	C4 VERIFY formatierte PIN		
R4	OK	--->	C5 READ RECORD EF_ID (CLA = '00', SFI '19', AC=ALW)		
		--->	A5 CID prüfen und spei- chern		
		<---	C6 READ RECORD EF_SEQ (CLA = '00', SFI '1C', AC=ALW)		
R6	Sequenznummer (SEQ)	--->	A6 SEQ speichern		
		<---	C7 READ RECORD EF_BNK (CLA = '00', SFI '1A', AC=ALW)		
R7	Bankverbindung	--->	A7 Daten prüfen und spei- chern		

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 78	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Chipapplikation für DDV

VIII.8.4.2 Nachricht generieren

Dieser Teil des Gesamtablaufs ist nur insofern chipkartenrelevant, als Bankverbindungsdaten, die für die Auftragsgenerierung benötigt werden, aus der Chipkarte entnommen werden. Für die folgende Ablaufbeschreibung wird angenommen, daß die Anwendung bereits HBCI-Aufträge generiert und zu HBCI-Nachrichten, bestehend aus Nachrichtenkopf, HBCI-Nutzdaten und Nachrichtenabschluß, zusammengefaßt hat.

Die so generierten HBCI-Nachrichten müssen jetzt ggf. noch kryptographisch gesichert werden, d.h. es werden Segmente für die elektronische(n) Signatur(en) und für die Verschlüsselung entsprechend den HBCI-Spezifikationen eingefügt.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Chipapplikation für DDV	Stand: 02.02.1998	Seite: 79

VIII.8.4.3 Nachricht signieren

Die folgenden Abläufe können offline, d.h. außerhalb des Übertragungsdialogs vollzogen werden. Dies gilt für alle Nachrichten mit Ausnahme der Dialoginitialisierung. Der Grund besteht darin, daß für die Absicherung aller Kreditinstitutsnachrichten der Schlüssel des Senders der Dialoginitialisierungsnachricht erforderlich ist. Daher muß auch die Chipkarte des Senders während des gesamten Dialogs im Endgerät stecken.

Die Abläufe für die Signatur der Dialoginitialisierungsnachricht sind grundsätzlich identisch mit den im folgenden beschriebenen Abläufen für die Signatur von Auftragsnachrichten. Da aber für die Dialoginitialisierung anwendungsseitig noch weitere Chipkartendaten (Benutzerkennung, Dialog-ID, Kommunikationszugang etc.) benötigt werden, wird der komplette Ablauf einschließlich der Signatur der Dialoginitialisierung im Abschnitt VIII.8.4.5 "Übertragung von HBCI-Nachrichten" noch einmal beschrieben.

MFC			Endgerät/Gateway		Kreditinstitut	
			A1	Sequenzzähler (Signatur-ID) SEQ inkrementieren		
R2	OK	<--- --->	C2	SELECT EF_KEYD		
			C3	READ RECORD EF_KEYD (CLA='00', P1='01', P2='04')		
R3	Datensatz	<--- --->	A4	Signaturkopf aufbauen und in HBCI-Nachricht einfügen		
			A5	Daten (Signaturkopf, HBCI-Nutzdaten) für MAC-Berechnung bereitstellen		
		<-->	M6	MAC über Daten berechnen (siehe VIII.8.5.1)		
		<--- --->	C7	UPDATE RECORD EF_SEQ mit SEQ (SFI '1C', AC=PWD)		
R7	OK		A8	Signaturabschluß aufbauen und in HBCI-Nachricht einfügen		
			A9	ggf. A1 bis A8 für weitere Nachrichten wiederholen		
			A10	signierte HBCI-Nachrichten zur Weiterverarbeitung speichern		
			A11	ggf. Startdialog und A1 bis A10 für Mehrfachsignaturen wiederholen		

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 80	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Chipapplikation für DDV

VIII.8.4.4 Nachricht verschlüsseln

MFC			Endgerät/Gateway		Kreditinstitut	
R1	OK	<--- --->	C1	SELECT EF_AUTD		
R2	Datensatz	<--- --->	C2	READ RECORD EF_AUTD (CLA='00', P1='01', P2='04')		
			A3	Daten (HBCI-Nutz- daten und ggf. Signa- turkopf/-abschluß) für die Verschlüsselung bereitstellen		
		<-->	M4	Daten und Nachrich- tenschlüssel ver- schlüsseln (siehe VIII.8.5.3)		
			A5	Verschlüsselungskopf aufbauen und in HBCI-Nachricht einfü- gen		
			A6	Verschlüsselte Daten als Binärdaten in HBCI-Nachricht einfü- gen		
			A7	ggf. A1 bis A6 für weitere Nachrichten wiederholen		
			A8	Verschlüsselte und si- gnierte HBCI-Mel- dungen zur weiteren Bearbeitung speichern		

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Chipapplikation für DDV	Stand: 02.02.1998	Seite: 81

VIII.8.4.5 Übertragungsdialog

MFC		Endgerät/Gateway		Kreditinstitut	
		A1	Sequenzzähler (Signatur-ID) SEQ inkrementieren		
		A2	Aus der bereits gelesenen Bankverbindung (EF_BNK) die Benutzerkennung, ... aus Bankverbindung EF_BNK ermitteln		
		A3	Dialoginitialisierungsnachricht aufbauen		
		A4	Signaturkopf aufbauen und in HBCI-Nachricht einfügen		
		A5	Daten (Signaturkopf, HBCI-Nutzdaten) für MAC-Berechnung bereitstellen		
		<--> M6	MAC über Daten berechnen (siehe VIII.8.5.1)		
		<--- C7	UPDATE RECORD EF_SEQ mit SEQ (SFI '1C', AC=PWD)		
R7	OK	--->			
		A8	Signaturabschluß aufbauen und in HBCI-Nachricht einfügen		
		A9	Kommunikationszugang aus Bankverbindung herstellen		
		C10	Nachricht (beginnend mit Dialoginitialisierungsnachricht) senden	---->	
		A11	falls Antwortnachricht verschlüsselt: Daten (Binärdaten nach dem Signaturkopf) und $d * K_{ENC}(KS)$ aus dem Signaturkopf für die Entschlüsselung bereitstellen	<---	R10 Antwortnachricht senden
		<--> M12	Daten entschlüsseln (siehe VIII.8.5.4)		
			falls Kreditinstitutsnachricht signiert:		
		A13	Daten (Signaturkopf, Nutzdaten) und Re-		

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 82	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Chipapplikation für DDV

MFC		Endgerät/Gateway		Kreditinstitut	
			ferenz-MAC für MAC-Prüfung bereit- stellen		
		M14	MAC über Daten und Referenz-MAC prü- fen (siehe VIII.8.5.2)		
		A15	C10 bis M14 für alle weiteren HBCI-Nach- richten wiederholen		

Die Benutzerkennung wird in die DEG „Schlüsselname“ (Kap. VI.5.1.1) eingestellt.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Chipapplikation für DDV	Stand: 02.02.1998	Seite: 83

VIII.8.5 Makros

VIII.8.5.1 MAC-Berechnung

MFC		Endgerät/Gateway		Kreditinstitut	
		A1	Hashwert HASH über Daten berechnen (RIPEMD160)		
		A2	HASH zerlegen in HASH_L (die linken 8 Byte von HASH) und HASH_R (die restlichen 12 Byte)		
R3	OK	<--- C3	UPDATE RECORD EF_MAC mit HASH_R (SFI '1B', AC=PWD)		
R4	OK	---> C4	PUT DATA mit HASH_L		
R5	Daten aus EF_MAC mit CFB-64 MAC über HASH_R (identisch mit CBC-MAC über HASH)	<--- C5	READ RECORD EF_MAC (CLA = '04', SFI '1B', AC=PRO)		
		---> A5	MAC zwischenspeichern		

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 84	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Chipapplikation für DDV

VIII.8.5.2 MAC-Prüfung

MFC		Endgerät/Gateway		Kreditinstitut	
		A1	Hashwert HASH über Daten berechnen (RIPEMD160)		
		A2	HASH zerlegen in HASH_L (die linken 8 Byte von HASH) und HASH_R (die restlichen 12 Byte)		
R3	OK	<--- C3	UPDATE RECORD EF_MAC mit HASH_R (SFI '1B', AC=PWD)		
R4	OK	---> C4	PUT DATA mit HASH_L		
R5	Daten aus EF_MAC mit CFB-64 MAC über HASH_R (identisch mit CBC-MAC über HASH)	<--- C5	READ RECORD EF_MAC (CLA = '04', SFI '1B', AC=PRO)		
		---> A5	MAC aus Kreditinstitutsnachricht mit MAC der Chipkarte vergleichen		

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Chipapplikation für DDV	Stand: 02.02.1998	Seite: 85

VIII.8.5.3 Verschlüsselung

MFC			Endgerät/Gateway		Kreditinstitut	
R1	OK	<--- --->	C1	SELECT EF_AUTD		
R2	Datensatz	<--- --->	C2	READ RECORD EF_AUTD (CLA='00', P1='01', P2='04')		
R3	RND	<--- --->	C3	GET CHALLENGE		
			A3	RND als Nachrichtenschlüssel-Hälfte KS_L speichern		
R4	$e * K_{ENC}(KS_L)$	<--- --->	C4	INTERNAL AUTHENTICATE mit KS_L		
			A4	$e * K_{ENC}(KS_L)$ speichern		
R5	RND	<--- --->	C5	GET CHALLENGE		
			A5	RND als Nachrichtenschlüssel-Hälfte KS_R speichern		
R6	$e * K_{ENC}(KS_R)$	<--- --->	C6	INTERNAL AUTHENTICATE mit KS_R		
			A6	$e * K_{ENC}(KS_R)$ speichern		
			A7	$e * K_{ENC}(KS_L)$ mit $e * K_{ENC}(KS_R)$ zu $e * K_{ENC}(KS)$ konkatenieren		
			A8	$e * K_{ENC}(KS)$ speichern		
			A9	KS_L mit KS_R zu KS konkatenieren		
			A10	Daten mit Schlüssel KS verschlüsseln (Triple-DES CBC- Mode, IV=0, X9.23 Padding)		

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 86	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Chipapplikation für DDV

VIII.8.5.4 Entschlüsselung

MFC		Endgerät/Gateway		Kreditinstitut	
		A1	$d * K_{ENC}(KS)$ in die zwei Hälften $d * K_{ENC}(KS_L)$ und $d * K_{ENC}(KS_R)$ zerlegen		
R2	KS_L	<--- C2	INTERNAL AUTHENTICATE mit $d * K_{ENC}(KS_L)$		
		---> A2	KS_L zwischenspeichern		
R3	KS_R	<--- C3	INTERNAL AUTHENTICATE mit $d * K_{ENC}(KS_R)$		
		---> A3	KS_R zwischenspeichern		
		A4	KS_L mit KS_R zu KS konkatenieren		
		A5	Daten mit Schlüssel KS entschlüsseln (Triple-DES CBC-Mode, IV=0, X9.23 Padding)		

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Chipapplikation für DDV	Stand: 02.02.1998	Seite: 87

VIII.8.6 Beispiel für einen HBCI-Dialog mit Chipkarte

Es werden für die Signatur von Nachrichten und für die Verschlüsselung von Nachrichtenschlüsseln unterschiedliche Schlüssel verwendet, wobei in der Chipkarte kartenspezifische Schlüssel gespeichert sind, die sich dynamisch aus den Kartenidentifikationsdaten und einem Key Generating Key herleiten lassen. Die Key Generating Keys sind ZKA-weit einheitlich, um die Multibankfähigkeit der Anwendung zu gewährleisten.

Der Key Generating Key für die Signatur von Nachrichten wird mit KGK_{DSG} und der Key Generating Key für die Verschlüsselung des Nachrichtenschlüssels mit KGK_{ENC} bezeichnet.

Das nachfolgende Beispiel soll verdeutlichen, wie die einzelnen Kunden-/Kreditinstitutsnachrichten abgesichert werden.

◆ Parameter für das Beispiel

Benutzer	User A	User B	User C	User D
Benutzerrechte	Signieren	Signieren	Verschlüsseln	Dialog
aus Identifikationsdaten	CID_A	CID_B	CID_C	CID_D
und KGK_{ENC} wird dynamisch generiert	$A_{K_{ENC}}$	$B_{K_{ENC}}$	$C_{K_{ENC}}$	$D_{K_{ENC}}$
und KGK_{DSG} wird dynamisch generiert	$A_{K_{DSG}}$	$B_{K_{DSG}}$	$C_{K_{DSG}}$	$D_{K_{DSG}}$
Signatur-ID im EF_SEQ (vorher)	A	B	C	D
Signatur-ID im EF_SEQ (nachher)	A + 2	B + 2	C	D + 2

◆ Absicherung von Nachrichten - Beispieldialog mit unterschiedlichen Benutzerrechten

		1. Signatur		2. Signatur		Verschlüsselung
		KEY	SEQ	KEY	SEQ	
Dialoginitialisierungsnachricht	Anfrage	$D_{K_{DSG}}$	D+1	-	-	-
	Antwort	$D_{K_{DSG}}$	D+1	-	-	-
1. Auftragsnachricht (Überweisung) (Signatur von User A erforderlich)	Anfrage	$A_{K_{DSG}}$	A+1	-	-	$C_{K_{ENC}}$
	Antwort	$D_{K_{DSG}}$	D+1	-	-	$D_{K_{ENC}}$
2. Auftragsnachricht (Überweisung) (Signatur von User B erforderlich)	Anfrage	$B_{K_{DSG}}$	B+1	-	-	$C_{K_{ENC}}$
	Antwort	$D_{K_{DSG}}$	D+1	-	-	$D_{K_{ENC}}$
3. Auftragsnachricht (Überweisung) (Signatur von User A und User B erforderlich)	Anfrage	$A_{K_{DSG}}$	A+2	$B_{K_{DSG}}$	B+2	$C_{K_{ENC}}$
	Antwort	$D_{K_{DSG}}$	D+1	-	-	$D_{K_{ENC}}$
4. Auftragsnachricht (Umsätze)	Anfrage	$D_{K_{DSG}}$	D+2	-	-	-
	Antwort	$D_{K_{DSG}}$	D+2	-	-	$D_{K_{ENC}}$

Die Signatur-IDs bei den Kunden- und Kreditinstitutsnachrichten sind identisch und stimmen mit der Signatur-ID in den Antwortnachrichten überein. Die Dialog-ID ist für alle Nachrichten konstant und wird aus dem Signaturzähler des Users D zum Zeitpunkt der Dialoginitialisierung abgeleitet.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 89

VIII.9 Verwendete Finanzdatenformate

VIII.9.1 DTAUS

◆ Zeichencode¹

Zugelassen sind

- die numerischen Zeichen 0 bis 9 (X'30' - X'39')
- die Großbuchstaben A - Z (X'41' - X'5A')
- die Sonderzeichen

Leerzeichen	„ „	= X'20'
Punkt	„.“	= X'2E'
Komma	„,“	= X'2C'
Kaufmännisch „und“	„&“	= X'26'
Trennstrich	„-“	= X'2D'
Plus-Zeichen	„+“	= X'2B'
Stern	„*“	= X'2A'
Prozent-Zeichen	„%“	= X'25'
Schrägstrich	„/“	= X'2F'
Dollar	„\$“	= X'24'

- sowie die Umlaute Ä, Ö, Ü und das ß. Hierfür gelten die Codierungen „Ä“ = X'5B', „Ö“ = X'5C', „Ü“ = X'5D', „ß“ = X'7E'.

Für den richtigen Ausdruck davon abweichender Zeichen übernehmen die Kreditinstitute keine Haftung.

Das Kreditinstitut kann Kleinbuchstaben in Datensätzen in Großbuchstaben konvertieren oder diese Datensätze an den Einreicher zurückgeben; unzulässige Sonderzeichen kann es in Leerzeichen (Blanks) konvertieren.

◆ Dateiaufbau

Die logische Datei ist wie folgt aufzubauen:

Datensatz A = Datei-Vorsatz

Datensatz C = Zahlungsaustauschsatz

Datensatz E = Datei-Nachsatz

Eine logische Datei darf nur Gutschriften oder nur Lastschriften enthalten.

¹ Codierungen gemäß DIN 66003 (Ausgabe Juni 1974), Code Tabelle 2, Deutsche Referenz-Version.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 90	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

◆ Datensatz A (Datei-Vorsatz)

Der Datensatz A enthält den Dateiabsender und -empfänger, er ist je logische Datei nur einmal vorhanden. Der Datensatz A ist 128 Byte lang.

Feld	Länge in Bytes	Daten- format ²	Inhalt	Erläuterung
1	4	numerisch	Satzlänge	'0128'
2	1	alpha	Satzart	Konstante "A"
3	2	alpha	Kennzeichen "GK" bzw. "LK"	Hinweis auf Gutschriften (=G) bzw. Lastschriften (=L); (K=Kundendatei)
4	8	numerisch	Bankleitzahl	Bankleitzahl des Kreditinstituts (Dateiempfänger)
5	8	numerisch	X'30'	-
6	27	alpha	Kundenname	Dateiabsender
7	6	numerisch	Datum	Dateierstellungsdatum (TTMMJJ)
8	4	-----	X'20'	
9	10	numerisch	Kontonummer	Empfänger/Absender Kunde, max 10 Stellen. Über dieses Konto wird der Gegenwert verrechnet.
10	10	numerisch	Referenznummer des Einreichers	Angabe freigestellt
11a	15	alpha	X'20'	Reserve
11b ³	8	alpha	Ausführungsdatum (TTMMJJJJ)	Angabe freigestellt. Nicht jünger als Dateierstellungsdatum (Feld A7), jedoch höchstens 15 Kalendertage über Erstellungsdatum aus Feld A7. Soweit in diesem Datenfeld ein Ausführungstermin angegeben wird, ist zu beachten, daß der in den Sonderbedingungen genannte Nachweiszeitraum von mindestens 10 Kalendertagen erst ab dem genannten Ausführungstermin zu berechnen ist.
11c	24	alpha	X'20'	Reserve
12	1	alpha	Währungskennzeichen	X'20' = DM 1 = Euro (ab dem Start der Stufe 3 der EWWU zulässig)
	128			

² alpha = alpha-numerische Daten (linksbündig, nicht belegte Stellen X'20')
numerisch = numerische Daten, ungepackt (rechtsbündig mit vorlaufenden Nullen X'30')

³ Belegung zulässig ab 20.11.1997

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 91

◆ Datensatz C (Zahlungsaustauschsatz)

Der Datensatz C enthält Einzelheiten über die auszuführenden Aufträge (Gutschriften bzw. Lastschriften). Er gliedert sich in einen konstanten und einen variablen Teil.

1. Konstanter Teil, 1. Satzabschnitt

Feld	Länge in Bytes	Datenformat	Inhalt	Erläuterung
1	4	numerisch	Satzlänge	konstanter Teil 187 Bytes + Erweiterungsteil(e) zu 29 Bytes, max. '0622' ⁴
2	1	alpha	Satzart	Konstante "C"
3	8	numerisch	Bankleitzahl	erstbeteiligtes Kreditinstitut, freigestellt
4	8	numerisch	Bankleitzahl	endbegünstigtes Kreditinstitut/Zahlstelle
5	10	numerisch	Kontonummer	Überweisungsempfänger/Zahlungspflichtiger, rechtsbündig
6	13	numerisch	wenn nicht genutzt: Nullen	Das Feld C 6 kann wie folgt belegt werden: 1. Byte = 0 2.-12. Byte = Interne Kundennummer oder Nullen 13. Byte = 0 Diese vom Kunden ggf. angegebene interne Nummer wird von den erstbeauftragten Instituten/den ersten Inkassostellen bis zum endbegünstigten Institut/zur Zahlstelle weitergeleitet. Die Weitergabe der internen Nummer an den Überweisungsempfänger/Zahlungspflichtigen ist dem endbegünstigten Institut/der Zahlstelle freigestellt.
7a	2	numerisch	Textschlüssel	Kennzeichnung der Zahlungsart und Textschüsselergänzungen gemäß Anlage
7b	3	numerisch	Textschüsselergänzung	
8	1	-	X'20'	bankinternes Feld
9	11	numerisch	Betrag in DM einschl. Nachkommastellen ⁵	rechtsbündig, nur belegt, wenn Auftragswährung in den Datenfeldern A12 und C17a = X'20'; sonst Nullen
10	8	numerisch	Bankleitzahl	erstbeauftragtes Institut / erste Inkassostelle
11	10	numerisch	Kontonummer	Auftraggeber/Zahlungsempfänger, rechtsbündig

⁴ Die nur zur Abgrenzung des jeweiligen Satzabschnitts dienenden Felder des variablen Teils eines Datensatzes (Felder C 23, C 32, C 41, C 50, C 53) sind somit in der Satzlängenangabe nicht zu berücksichtigen.

⁵ Bei der Umrechnung von DM in Euro und umgekehrt dürfen nicht mehr als je 11 Stellen (einschl. Nachkommastellen) entstehen. Mit Beginn der Stufe 3 der EWWU werden die konkreten Höchstgrenzen fixiert.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 92	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

Feld	Länge in Bytes	Daten- format	Inhalt	Erläuterung
12	11	numerisch	Betrag in Euro einschl. Nach- kommastellen ⁶	rechtsbündig, nur belegt, wenn Auftrags- währung in den Datenfeldern A12 und C17a = '1'; sonst Nullen
13	3	-	X '20'	Reserve
14a	27	alpha	Name	Überweisungsempfänger/Zahlungspflich- tiger, linksbündig
14b	8	-	X'20'	nur zur Abgrenzung des Satzabschnitts (darf keine Daten enthalten)
	128			

⁶ Erst ab dem Start der Stufe 3 der EWWU zulässig.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 93

1. Konstanter Teil, 2. Satzabschnitt

Feld	Länge in Bytes	Daten- format	Inhalt	Erläuterung
15	27	alpha	Name	Auftraggeber/Zahlungsempfänger (linksbündig), es sind möglichst kurze Bezeichnungen zu verwenden
16	27	alpha	Verwendungszweck	Es sind möglichst kurze Angaben zu machen. Am Anfang dieses Feldes sind linksbündig solche Angaben unterzubringen, auf die der Begünstigte bei Überweisungen möglicherweise zuzugreifen beabsichtigt (z.B. Bausparkontonummer, Versicherungsnummer, Rechnungsnummer) oder die der Zahlungsempfänger bei Lastschriften benötigt, falls die Zahlung als unbezahlt bzw. unanbringlich an ihn zurückgeleitet wird.
17a	1	alpha	Währungskennzeichen	X'20' = DM 1 = Euro (ab dem Start der Stufe 3 der EWWU zulässig)
17b	2	-	X'20'	Reserve
18	2	numerisch	Erweiterungskennzeichen	00 = es folgt kein Erweiterungsteil 01-15 = Anzahl der Erweiterungsteile

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 94	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

2. Variabler Teil, noch 2. Satzabschnitt

Der variable Teil bildet mit dem konstanten Teil eine Einheit. Er ist nur dann vorhanden, wenn die Datenfelder im konstanten Teil für die Aufnahme von Informationen nicht ausreichen. Maximal können bis zu 6 Satzabschnitte à 128 Bytes für den Datensatz C belegt sein. Es können vorkommen: 1 Erweiterungsteil für „Überweisungsempfänger“ bzw. „Zahlungspflichtiger“ (01), bis 13 Erweiterungsteile für „Verwendungszweck“ (alle 02) und 1 Erweiterungsteil für „Auftraggeber“ bzw. „Zahlungsempfänger“ (03).

Feld	Länge in Bytes	Datenformat	Inhalt	Erläuterung
19	2	numerisch	Kennzeichen des Erweiterungsteils	01 = Name des Überweisungsempfängers/Zahlungspflichtigen 02 = Verwendungszweck 03 = Name Auftraggeber bzw. Zahlungsempfänger
20	27	alpha	Überweisungsempfänger bzw. Zahlungspflichtiger/Verwendungszweck/Auftraggeber bzw. Zahlungsempfänger	Linksbündig. Bei Rücküberweisungen und Rücklastschriften kann der Inhalt von Erweiterungsteilen von den Banken auf dem Beleg unter „Verwendungszweck“ grundsätzlich nicht angegeben werden. Alle für die Bearbeitung derartiger Rückbelege erforderlichen Verwendungszweckangaben sind daher vom Zahlungsempfänger bzw. Auftraggeber im konstanten Teil des Datensatzes C unterzubringen (siehe Erläuterungen zu Feld C 16).
21	2	numerisch	Kennzeichen des Erweiterungsteils	(wie Feld 19)
22	27	alpha	Daten Erweiterungsteil	(wie Feld 20)
23	11	-	X'20'	nur zur Begrenzung des Satzabschnitts (keine Berücksichtigung für die Satzlängenangabe im Feld C 1)
	128			

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 95

2. Variabler Teil, 3. Satzabschnitt⁷

Feld	Länge in Bytes	Daten- format	Inhalt	Erläuterung
24	2	numerisch	Kennzeichen des Erweite- rungsteils	(wie Feld 19)
25	27	alpha	Daten des Er- weiterungsteils	(wie Feld 20)
26	2	numerisch	Kennzeichen des Erweite- rungsteils	(wie Feld 19)
27	27	alpha	Daten des Er- weiterungsteils	(wie Feld 20)
28	2	numerisch	Kennzeichen des Erweite- rungsteils	(wie Feld 19)
29	27	alpha	Daten des Er- weiterungsteils	(wie Feld 20)
30	2	numerisch	Kennzeichen des Erweite- rungsteils	(wie Feld 19)
31	27	alpha	Daten des Er- weiterungsteils	(wie Feld 20)
32	12	-	X'20'	nur zur Abgrenzung des Satzabschnitts (keine Berücksichtigung für die Satzlängen- angabe im Feld C 1)
	128			

⁷ Für darüber hinaus noch erforderliche Erweiterungsteile stehen der 4.-6. Satzabschnitt noch zur Verfügung. Der Aufbau des 4. und 5. Satzabschnitts entspricht dem des 3. Satzabschnitts. Satzabschnitt 6 enthält nur einen Erweiterungsteil.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 96	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

♦ **Datensatz E (Datei-Nachsatz)**

Der Datensatz E dient der Abstimmung; er ist je logische Datei nur einmal vorhanden.

Feld	Länge in Bytes	Daten- format	Inhalt	Erläuterungen
1	4	numerisch	Satzlänge	'0128'
2	1	alpha	Satzart	Konstante "E"
3	5	-	X'20'	Reserve
4	7	numerisch	Anzahl der Datensätze C	Abstimm-Unterlagen
5	13	numerisch	Summe der DM-Beträge aus Feld 9 der Datensätze C	Abstimm-Unterlage, wenn Auftragswährung in den Datenfeldern A12 und C17a = X'20', sonst Nullen
6	17	numerisch	Summe der Kontonummern aus Feld 5 der Datensätze C	Abstimm-Unterlagen
7	17	numerisch	Summe der Bankleitzahlen aus Feld 4 der Datensätze C	Abstimm-Unterlagen
8	13	numerisch	Summe der Euro-Beträge aus Feld 12 der Datensätze C	Abstimm-Unterlage, wenn Auftragswährung in den Datenfeldern A12 und C17a = '1', sonst Nullen
9	51	-	X'20'	nur zur Abgrenzung des Satzabschnitts
	128			

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 97

◆ Anlage: Erläuterungen zu Feld 7a und 7b des Datensatzes C

Zur Kennzeichnung der Zahlungsart sind vom Kreditgewerbe einheitliche Textschlüssel festgelegt worden. Soweit für einzelne Gutschriftsarten besondere Textschlüssel vorgesehen wurden, sind diese unbedingt zu verwenden. Dies gilt vor allem für Lohn-, Gehalts- oder Rentengutschriften (Textschlüssel „53“) und für vermögenswirksame Leistungen (Textschlüssel „54“). Öffentliche Kassen können die von ihnen überwiesenen Löhne und Gehälter mit dem Textschlüssel '56' kennzeichnen.

Folgende Belegungen der Datenfelder 7a und 7b können vorkommen:

Kundenseitig: (Kennzeichen „GK“ bzw. „LK“ in Feld 3 des Datensatzes A)

Textschlüssel Feld 7a	Textschlüssel- ergänzung Feld 7b	Erläuterung	Inhalt des Datenfeldes 7
04	000 ^A	Lastschrift (Abbuchungsauftragsverfahren)	'04000'
05	000 ^A	Lastschrift (Einzugsermächtigungsverfahren)	'05000'
51	000 ^A	Überweisungsgutschrift (z.B. kommerzielle Zahlung)	'51000'
53	000 ^A	Lohn-, Gehalts-, Renten-Gutschrift	'53000'
54	XXJ ^C	Vermögenswirksame Leistung (VL)	'54XXJ'
56	000	Überweisung öffentlicher Kassen	'56000'
67	000 ^A	Überweisungsgutschrift mit prüfzifferge- scherten Zuordnungsdaten (BZÜ-Überweisung)	'67000'
69	000 ^A	Gutschrift einer Spendenüberweisung	'69000'

^A Sofern es sich bei dem Auftraggeber der Zahlung/Zahlungsempfänger um einen Gebietsfremden im Sinne der Außenwirtschaftsverordnung handelt, sollte die Textschlüsselergänzung „000“ durch „888“ ersetzt werden.

^C Die Buchstaben „XX“ sind wahlweise durch „00“ oder durch den jeweiligen %-Satz der Sparzulage, der Buchstabe „J“ durch die letzte Ziffer des Jahres, für das die Leistung gelten soll, zu ersetzen. Beispiel: Bei einer Zahlung für 1997 mit 10%iger Sparzulage lautet die korrekte Belegung des Datenfeldes 7: „54007“ oder „54107“.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 98	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

♦ **Anlage: Kontrollmaßnahmen (Plausibilitäts- und Feldinhaltsprüfungen)**

Die Datensätze C sind wie folgt zu prüfen:

Feld	Inhalt	Datenformat
Bankleitzahl des endbegünstigten Kreditinstituts/der Zahlstelle (Feld C 4)	auf Existenz der Bankleitzahl lt. Bankleitzahlenverzeichnis der Deutschen Bundesbank, erste Stelle ungleich 0 oder 9	numerisch
Kontonummer des Überweisungsempfängers/Zahlungspflichtigen (Feld C 5)	ungleich Null	numerisch
interne Kundennummer (Feld C 6)	1. Byte gleich Null	numerisch
Textschlüssel - Lastschriften - Gutschriften (Feld C 7a)	- gleich 04, 05 - gleich 51-59, 67-69	numerisch
Betrag (Feld C 9)	ungleich Null	numerisch
Bankleitzahl des erstbeauftragten Kreditinstitutes/der ersten Inkassostelle (Feld C 10)	1. Stelle ungleich 0 oder 9	numerisch
Kontonummer des Auftraggebers/Zahlungsempfängers (Feld C 11)	ungleich Null	numerisch
Name des Überweisungsempfängers/Zahlungspflichtigen (Feld C 14a)	ungleich X'20'	alphanumerisch
Name des Auftraggebers/Zahlungsempfängers (Feld C 15)	ungleich X'20'	alphanumerisch
Erweiterungskennzeichen (Feld C 18)	gleich 00-15	numerisch
Kennzeichen des Erweiterungsteils (Feld C 19; C 21; C 24; C 26 usw., variabler Teil)	gleich 01, 02 oder 03 in aufsteigender Reihenfolge max. 1 mal 01 max. 13 mal 02 max. 1 mal 03	numerisch

Die Kontrollsummen aus der Addition der Stückzahl der Datensätze C, der Felder „Betrag“ (C 9), „Kontonummer des Überweisungsempfängers/Zahlungspflichtigen“ (C 5) und „Bankleitzahl des endbegünstigten Kreditinstituts/der Zahlstelle“ (C 4) müssen mit den Angaben im Datensatz E übereinstimmen.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 99

Zusätzlich ist bei Unterstützung des EWWU-Formats (Segmentversion 3) zu prüfen:

Feld	Inhalt	Datenformat
Betrag (Feld C 9)	ungleich Null bei X'20' in den Datenfeldern A12 und C17a oder gleich Null bei '1' in den Datenfeldern A12 und C17a (ab dem Start der Stufe 3 der EWWU zulässig)	numerisch
Betrag (Feld C 12)	ungleich Null bei '1' in den Datenfeldern A12 und C17a (ab dem Start der Stufe 3 der EWWU zulässig) oder gleich Null bei X'20' in den Datenfeldern A12 und C17a	numerisch
Währungskennzeichen (Feld C 17a)	gleich X'20', wenn Datenfeld A12 = X'20' gleich '1', wenn Datenfeld A12 = '1' (ab dem Start der Stufe 3 der EWWU zulässig)	alphanumerisch

Die Kontrollsummen aus der Addition der Stückzahl der Datensätze C, der Felder „Betrag“ (C 9 und C12), „Kontonummer des Überweisungsempfängers/Zahlungspflichtigen“ (C 5) und „Bankleitzahl des endbegünstigten Kreditinstituts/der Zahlstelle“ (C 4) müssen mit den Angaben im Datensatz E übereinstimmen.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 100	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

VIII.9.2 DTAZV

Eine Datenübertragung darf nur eine Datei mit Zahlungsaufträgen im Außenwirtschaftsverkehr enthalten, d.h. Q- und Z-Satz können nur einmal vorkommen.

◆ Zeichencode⁸

Zugelassen sind

- die numerischen Zeichen 0 bis 9 (X'30' - X'39')
- die Großbuchstaben A - Z (X'41' - X'5A')
- die Sonderzeichen

Leerzeichen	„ „	= X'20'
Punkt	„.“	= X'2E'
Komma	„,“	= X'2C'
kaufmännisch „und“	„&“	= X'26' [*]
Trennstrich	„-“	= X'2D'
Schrägstrich	„/“	= X'2F'
Plus-Zeichen	„+“	= X'2B'
Stern	„*“	= X'2A' [*]
Dollar-Zeichen	„\$“	= X'24' [*]
Prozent-Zeichen	„%“	= X'25' [*]

Die Umlaute Ä, Ö, Ü sind wie AE, OE, UE aufzuzeichnen, das ß wie SS.

Für den richtigen Ausdruck davon abweichender Zeichen übernehmen die Kreditinstitute keine Haftung.

Das Kreditinstitut kann Kleinbuchstaben in Datensätzen in Großbuchstaben konvertieren oder diese Datensätze an den Einreicher zurückgeben; unzulässige Sonderzeichen kann es in Leerzeichen (Blanks) konvertieren.

◆ Dateiaufbau

Die logische Datei ist wie folgt aufzubauen:

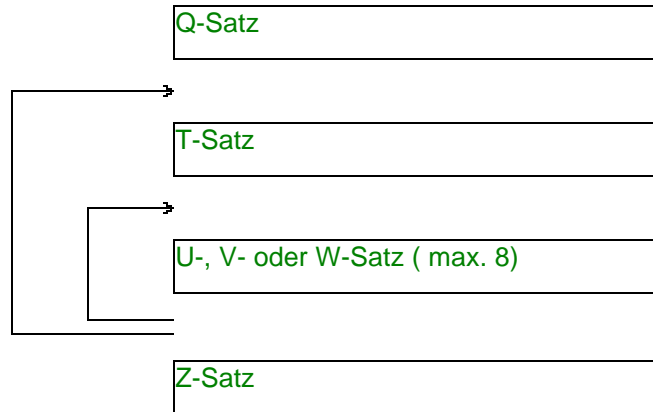
- Datensatz Q = Daten-Vorsatz mit 256 Byte
- Datensatz T = Einzelzahlungsauftrag mit 768 Byte
- Datensatz U = Meldedatensatz zur Wareneinfuhr mit 256 Byte
- Datensatz V = Meldedatensatz zum Transithandel mit 256 Byte
- Datensatz W = Meldedatensatz für Dienstleistungs-, Kapitalverkehr und Sonstiges mit 256 Byte
- Datensatz Z = Daten-Nachsatz mit 256 Byte

⁸ Codierungen gemäß DIN 66003 (Ausgabe Juni 1974), Code Tabelle 2, Deutsche Referenz-Version.

^{*} z.Zt. nicht zugelassen

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 101

Die Datensätze Q und Z gibt es nur einmal. Die restlichen Datensätze können beliebig oft vorkommen, ihre Reihenfolge ist lediglich durch ihren logischen Zusammenhang bestimmt und wird in der folgenden Abbildung schematisch dargestellt.



Es ist nicht zulässig, eine Datei auf mehrere Übertragungen aufzuteilen.

Abweichungen von dem Aufbau und den Spezifikationen bedürfen besonderer Absprachen.

Bei Verstößen, die zu einem Programmabbruch führen, insbesondere bei falscher Satzlänge und falschem Datenformat, ist der Empfänger berechtigt, die gesamte Datei unbearbeitet zurückzusenden.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 102	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

◆ Datensatz Q (Datei-Vorsatz)

Der Vorsatz enthält kundenbezogene Informationen, die für die gesamte Datei Gültigkeit haben. Der Datensatz ist nur einmal pro logische Datei vorhanden.

Feld	Länge in Bytes	1. Stelle im Satz	Status	Format ⁹	Inhalt	Erläuterung
1	4	1	M	num	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlänge
2	1	5	M	alpha	Satzart	Konstante "Q"
3	8	6	M	num	Bankleitzahl	erstbeauftragtes Institut
4	10	14	M	num	Kundennummer	Ordnungsnummer gemäß Vereinbarung mit dem erstbeauftragten Institut (ggf. Kontonummer)
5	4 x 35	24	M	alpha	Auftraggeberdaten	Zeile 1 und 2: Name Zeile 3: Straße/Postfach Zeile 4: Ort Für automatisch durchzuleitende Zahlungen 1 x 35 Stellen
6	6	164	M	num	Erstellungsdatum	Format: JJMMTT
7	2	170	M	num	laufende Nummer	laufende Tagesnummer
8	6	172	M	num	Ausführungstermin	Format: JJMMTT; nicht jünger als Erstellungsdatum (Feld Q 6), jedoch höchstens 15 Kalendertage über Erstellungsdatum aus Feld Q 6
9	1	178	M	alpha	Weiterleitung an die Meldebehörde	Soll das dateiempfangende Institut Meldedaten zu den nachfolgenden Zahlungsaufträgen an die Bundesbank weiterleiten? (siehe Erläuterungen im Anhang 3) 'J' Ja 'N' Nein
10	2	179	M/K	num	Bundesland-Nummer	Zwingend belegt, wenn Meldedaten zu den Zahlungsaufträgen an die Bundesbank weitergeleitet werden sollen. ('J' in Feld Q 9)
11	8	181	M/K	num	Firmennummer / BLZ des Auftraggebers	siehe Erläuterungen Feld Q 10
12	68	189	M	alpha	Leerzeichen	Reserve
	256					

⁹ alpha = alpha-numerische Daten (linksbündig, nicht belegte Stellen X'20')
num = numerische Daten, ungepackt (rechtsbündig, nicht belegte Stellen: Nullen)

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 103

◆ Datensatz T (Einzeldatensatz)

Der Einzeldatensatz enthält Informationen über den auszuführenden Transferauftrag.

Feld	Länge in Bytes	1. Stelle im Satz	Status	Format	Inhalt	Erläuterung
1	4	1	M	num	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlänge
2	1	5	M	alpha	Satzart	Konstante "T"
3	8	6	M	num	Bankleitzahl	BLZ der kontoführenden Stelle des mit dem Auftragswert (Feld T 4b) zu belastenden Kontos
4a	3	14	M	alpha	ISO-Währungscode	Für mit Auftragswert zu belastendes Konto.
4b	10	17	M	num	Kontonummer	Mit Auftragswert zu belastendes Konto
5	6	27	K	num	Ausführungstermin	Format: JJMMTT; nicht jünger als in Feld Q 8 angegebener Termin, jedoch höchstens 15 Kalendertage über Erstellungsdatum aus Feld Q 6
6	8	33	M/K	num	Bankleitzahl	BLZ der kontoführenden Stelle des mit Gebühren und Spesen zu belastenden Kontos (nur belegt, wenn abweichend von Feld T 3)
7a	3	41	M/K	alpha	ISO-Währungscode	Nur belegt, wenn abweichend von Feld T 4a: Mit Gebühren und Spesen zu belastendes Konto
7b	10	44	M/K	num	Kontonummer	Nur belegt, wenn abweichend von Feld T 4b: Mit Gebühren und Spesen zu belastendes Konto
8	11	54	K	alpha	SWIFT-Adresse der Bank des Begünstigten oder sonstige Identifikation, z.B. Chip-ID	Belegung rechtsbündig, nicht belegte Stellen mit '/' ausfüllen, sofern die Zahlung an ein deutsches Kreditinstitut erfolgt, alternativ auch die BLZ des Begünstigten, wobei dieser drei Schrägstriche voranzustellen sind.
9a	3	65	M/K	num	Länderkennziffer Bank des Begünstigten	Länderschlüssel gemäß Länderverzeichnis für die Zahlungsbilanzstatistik (s. Anlage) (nur belegt, wenn Feld T 8 nicht belegt)
9b	4 x 35	68	M/K	alpha	Anschrift der Bank des Begünstigten	nur zu belegen, wenn Feld T 8 nicht mit SWIFT-Adresse belegt, bzw. - bei Zahlungen an ein deutsches Kreditinstitut - mit BLZ belegt; sofern nicht bekannt, Konstante „unbekannt“ Zeile 1 und 2: Name Zeile 3: Straße

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 104	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

Feld	Länge in Bytes	1. Stelle im Satz	Status	Format	Inhalt	Erläuterung
						Zeile 4: Ort/Land
10a	3	208	M	num	Länderkennziffer Land des Begünstigten bzw. Scheckempfängers	Länderschlüssel gemäß Länderverzeichnis für die Zahlungsbilanzstatistik (s. Anlage)
10b	4 x 35	211	M	alpha	Begünstigter bzw. Scheckempfänger	Bei Zahlungsauftrag: Begünstigter Bei Scheckziehung: Scheckempfänger Zeile 1 und 2: Name Zeile 3: Straße Zeile 4: Ort/Land
11	2 x 35	351	K	alpha	Ordervermerk	Nur belegt bei Scheckziehung (20-23, 30-33 in Feld T 22) und Abweichung vom Inhalt der Zeilen 1 und 2 des Feldes T 10b
12	35	421	K	alpha	Kontonummer bzw. IBAN	Begünstigtenkonto, linksbündig mit Schrägstrich beginnend.
13	3	456	M	alpha	Auftragswährung	ISO-Code der zu zahlenden Währung (wenn die Auftragswährung ungleich DM oder Euro ist, muß sie der Währung des mit dem Auftragswert zu belastenden Kontos entsprechen, es sei denn, das mit dem Auftragswert zu belastende Konto ist ein DM- oder Euro-Konto) ¹⁰
14a	14	459	M	num	Betrag (Vorkommastellen)	rechtsbündig
14b	3	473	M	num	Betrag (Nachkommastellen)	linksbündig
15	4 x 35	476	K	alpha	Verwendungszweck	
16	2	616	K	num	Weisungsschlüssel 1 (gem. Anhang 2)	
17	2	618	K	num	Weisungsschlüssel 2 (gem. Anhang 2)	
18	2	620	M/K	num	Weisungsschlüssel 3 (gem. Anhang 2)	Ab Beginn der 3. Stufe der Währungsunion zu belegen mit einer Kennzeichnung für die Währung, in der die Beträge in den Datensätzen U, V und W angegeben werden, falls diese Währung nicht DM ist: '95' Auftragswährung (vgl. Feld T13)
19	2	622	M/K	num	Weisungsschlüssel 4 (gem. Anhang 1a und 2)	Für die Weisung „DM-Gegenwertzahlung“ bzw. „Euro-Gegenwertzahlung“ siehe Anhang 1a ¹¹

¹⁰ Zahlungen in Euro sind erst ab Beginn der 3. Stufe der EWWU zulässig.

¹¹ Zahlungen in Euro sind erst ab Beginn der 3. Stufe der EWWU zulässig.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 105

Feld	Länge in Bytes	1. Stelle im Satz	Status	Format	Inhalt	Erläuterung
20	25	624	K	alpha	Zusatzinformationen zum Weisungsschlüssel	z.B. Telex, Telefonnummer, Kabelanschrift
21	2	649	M	num	Kostenverrechnungsschlüssel	00 = Transfergebühren zu Lasten Auftraggeber/fremde Gebühren zu Lasten Begünstigter 01 = alle Gebühren zu Lasten Auftraggeber 02 = alle Gebühren zu Lasten Empfänger
22	2	651	M	num	Kennzeichnung der Zahlungsart	gemäß Anhang 1
23	27	653	K	alpha	Variabler Text nur für Auftraggeberabrechnung	Vom Auftraggeber frei belegbar (z.B. Referenz-Nr.). Wird nicht weitergeleitet; weiterzuleitende Informationen in Feld T 15 angeben.
24	35	680	M/K	alpha	Name und Telefonnummer sowie ggf. Stellvertretungsmeldung	Ansprechpartner beim Auftraggeber für evtl. interne Rückfragen der beauftragen Bank oder der Meldebehörde. Dahinter, wenn Auftraggeber nicht Zahlungspflichtiger ist: 'INVF', ohne Leerstellen gefolgt von: Bundesland-Nummer des Zahlungspflichtigen (2 stellig) und: Firmennummer bzw. BLZ des Zahlungspflichtigen (8-stellig)
25	1	715	K	num	Meldeschlüssel	nur belegt, wenn die Weiterleitung des Zahlungsauftrages an die Bundesbank auf die statistischen Angaben beschränkt werden soll; (dies sind die Datensätze U, V, W und Q (ohne Feld Q4) und die Felder 5, 13, 14a, 18, 19 und 24 - 27 des Datensatzes T). Belegung in diesem Falle : '1'
26	51	716	M	alpha	Leerzeichen	Reserve
27	2	767	M	num	Erweiterungskennzeichen	00 = es folgt kein Meldeteil 01-08 = Anzahl der Meldeteile à 256 Bytes
	768					

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 106	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

◆ **Datensatz U (Meldedatensatz für Wareneinfuhren)**

Feld	Länge in Bytes	1. Stelle im Satz	Status	Format	Inhalt	Erläuterung
1	4	1	M	num	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlänge
2	1	5	M	alpha	Satzart	Konstante „U“
3	7	6	K	alpha	Einkaufsland Wareneinfuhr	Kurzbezeichnung gemäß Länderverzeichnis für die Zahlungsbilanzstatistik (s. Anlage)
4	3	13	K	num	Länderschlüssel Einkaufsland Wareneinfuhr	gemäß Länderverzeichnis für die Zahlungsbilanzstatistik (s. Anlage)
5	12	16	M	num	Einkaufspreis der Wareneinfuhren (Vorkommastellen)	Angabe in DM, ab Beginn der 3. Stufe der Währungsunion auch Angabe in Auftragswährung möglich (Währungskennzeichnung in Feld T18).
6	229	28	M	alpha	Leerzeichen	Reserve
	256					

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 107

◆ **Datensatz V (Meldedatensatz für Transithandel)**

Feld	Länge in Bytes	1. Stelle im Satz	Status	Format	Inhalt	Erläuterung
1	4	1	M	num	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlänge
2	1	5	M	alpha	Satzart	Konstante „V“
3	27	6	M	alpha	Warenbezeichnung der eingekauften Transithandelsware	
4a	2	33	M	num	Kapitel-Nr. des Warenverzeichnisses für die eingekaufte Transithandelsware	gemäß Warenverzeichnis für die Außenhandelsstatistik
4b	7	35	M	num	„0000000“	Konstante „0000000“
5	7	42	M	alpha	Einkaufsland Transithandel	Kurzbezeichnung gemäß Länderverzeichnis für die Zahlungsbilanzstatistik (s. Anlage)
6	3	49	M	num	Länderschlüssel Einkaufsland Transithandel	gemäß Länderverzeichnis für die Zahlungsbilanzstatistik (s. Anlage)
7	12	52	M	num	Einkaufspreis Transithandel (Vorkommastellen)	Angabe in DM, ab Beginn der 3. Stufe der Währungsunion auch Angabe in Auftragswährung möglich (Währungskennzeichnung in Feld T18).
8	1	64	M	alpha	Verkauf der Transithandelsware an Gebietsfremde (durchgehandeltes Transithandelsgeschäft)	Ja (=J) bzw. Nein (=N)
9	1	65	M	alpha	Kennzeichnung Verkauf der Transithandelsware an Gebietsansässige (gebrochenes Transithandelsgeschäft)	Ja (=J) bzw. Nein (=N)
10	1	66	M	alpha	Kennzeichnung Transithandelsware unverkauft auf Lager im Inland	Ja (=J) bzw. Nein (=N)
11	1	67	M	alpha	Kennzeichnung Transithandelsware unverkauft auf Lager im Ausland	Ja (=J) bzw. Nein (=N)
12	27	68	M/K	alpha	Warenbezeichnung der verkauften Transithandelsware	nur belegt, wenn durchgehandelter Transithandel ('J' in Feld V8) und nicht identisch mit Feld V3

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 108	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

Feld	Länge in Bytes	1. Stelle im Satz	Status	Format	Inhalt	Erläuterung
13a	2	95	M/K	num	Kapitel-Nr. des Warenverzeichnisses für die verkaufte Transithandelsware	gemäß Warenverzeichnis für die Außenhandelsstatistik; nur belegt, wenn durchgehandelter Transithandel ('J' in Feld V8) und wenn Feld V13a nicht identisch mit Feld 4a
13b	7	97	M/K	num	„0000000“	Konstante „0000000“
14	4	104	M	alpha	Fälligkeit Verkaufserlös Transithandel	nur belegt, wenn durchgehandelter Transithandel ('J' in Feld V8), Format: JJMM
15	7	108	M/K	alpha	Käuferland Transithandel	Kurzbezeichnung gemäß Länderverzeichnis für die Zahlungsbilanzstatistik; nur belegt, wenn durchgehandelter Transithandel ('J' in Feld V8)
16	3	115	M/K	num	Länderschlüssel Käuferland	gemäß Länderverzeichnis für die Zahlungsbilanzstatistik; nur belegt, wenn durchgehandelter Transithandel ('J' in Feld V8)
17	12	118	M/K	num	Verkaufspreis Transithandel (Vorkommastellen)	nur belegt, wenn durchgehandelter Transithandel ('J' in Feld V8); Angabe in DM, ab Beginn der 3. Stufe der Währungsunion auch Angabe in Auftragswährung möglich (Währungskennzeichnung in Feld T18)
18	40	130	M/K	alpha	Ergänzungsangaben Transithandel	Name und Sitz des Nachkäufers bei gebrochenem Transithandel ('J' in Feld V9)
19	87	170	M	alpha	Leerzeichen	Reserve
	256					

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 109

♦ **Datensatz W (Meldedatensatz für sonstige Zahlungszwecke z.B.: Dienstleistungen, Kapitaltransaktionen)**

Feld	Länge in Bytes	1. Stelle im Satz	Status	Format	Inhalt	Erläuterung
1	4	1	M	num	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlänge
2	1	5	M	alpha	Satzart	Konstante „W“
3	1	6	M	num	Belegart	Dienstleistungen, Übertragungen = '2' Kapitaltransaktionen u. Kapitalerträge = '4'
4	3	7	M	num	Kennzahl	gemäß Leistungsverzeichnis (Anlage LV zur AWV)
5	7	10	M	alpha	Land	Kurzbezeichnung gemäß Länderverzeichnis für die Zahlungsbilanzstatistik (siehe Anhang 3, Abschnitt E)
6	3	17	M	num	Länderschlüssel	gemäß Länderverzeichnis für die Zahlungsbilanzstatistik (siehe Anhang 3, Abschnitt E)
7	7	20	M/K	alpha	Anlageland bei Kapitalverkehr	Kurzbezeichnung gemäß Länderverzeichnis für die Zahlungsbilanzstatistik ¹²
8	3	27	M/K	num	Länderschlüssel Anlageland	gemäß Länderverzeichnis für die Zahlungsbilanzstatistik ¹³
9	12	30	M	num	Betrag für Dienstleistungen, Kapitalverkehr, Sonstiges (Vorkommastellen)	Angabe in DM; Ab Beginn der 3. Stufe der Währungsunion auch Angabe in Auftragswährung möglich (Währungskennzeichnung in Feld T18)
10	140	42	M	alpha	nähere Angaben zur zugrundeliegenden Leistung	wichtige Einzelheiten des Grundgeschäfts
11	75	182	M	alpha	Leerzeichen	Reserve
	256					

¹² Kann ab sofort leer gelassen werden, wenn die Felder 5 und 6 gemäß Anhang 3, Abschnitt E, belegt sind.

¹³ Kann ab sofort leer gelassen werden, wenn die Felder 5 und 6 gemäß Anhang 3, Abschnitt E, belegt sind.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 110	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

◆ **Datensatz Z (Datei-Nachsatz)**

Der Nachsatz dient der Abstimmung. Er ist pro logische Datei nur einmal vorhanden.

Feld	Länge in Bytes	1. Stelle im Satz	Status	Format	Inhalt	Erläuterung
1	4	1	M	num	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlänge
2	1	5	M	alpha	Satzart	Konstante "Z"
3	15	6	M	num	Summe aller Beträge (nur Vorkommastellen)	Summe der Betragsangabe in Feld T 14a (über alle Währungen)
4	15	21	M	num	Anzahl der Datensätze 'T'	
5	221	36	M	alpha	Leerzeichen	Reserve
	256					

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 111

♦ Anhang 1: Schlüssel zur Kennzeichnung der Zahlungsart

1. zwischenbetrieblich festgelegt:

- 00 = Standardübermittlung (z.B. briefliche, SWIFT-Normal)
- 10 = Telex-Zahlung oder SWIFT-Eilig
- 20 = Scheckziehung, Versandform freigestellt
- 21 = Scheckziehung, Versandform per Einschreiben
- 22 = Scheckziehung, Versandform per Eilboten
- 23 = Scheckziehung, Versandform per Einschreiben/Eilboten
- 30 = Scheckziehung an Auftraggeber, Versandform freigestellt
- 31 = Scheckziehung an Auftraggeber, Versandform Einschreiben
- 32 = Scheckziehung an Auftraggeber, Versandform Eilboten
- 33 = Scheckziehung an Auftraggeber, Versandform Einschreiben/Eilboten

2. zwischenbetrieblich reserviert:

- 34
- .
- .
- zunächst frei
- .
- 49

3. innerbetrieblich:

- 50
- .
- .
- .
- 99

♦ Anhang 1a: Weisungsschlüssel für „DM- oder Euro-Gegenwertzahlungen“

Die Weisung „DM- oder Euro-Gegenwertzahlung“ kann nur im Feld T19 erteilt werden.

T19 = 90 = DM-Gegenwertzahlungen.

T19 = 91 = Euro-Gegenwertzahlungen.

Der in den Feldern T14a und T14b angegebene Betrag ist der DM- bzw. Euro-Betrag, der in die in Feld T13 angegebene Währung konvertiert und in dieser Währung an den Begünstigten bzw. Scheckempfänger gezahlt wird.

Eine DM-Gegenwertzahlung kann nur zu Lasten eines DM-Kontos und eine Euro-Gegenwertzahlung nur zu Lasten eines Euro-Kontos erfolgen.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 112	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

◆ Anhang 2: Weisungsschlüssel

Schlüssel	SWIFT-Abk.	Klartext
01	/BENONLY/	PAY TO BENEFICIARY ONLY ZAHLET BITTE NUR AN BEGÜNSTIGTEN
02	/CHEQUE/	PAY ONLY BY CHEQUE ZAHLET NUR MITTELS SCHECK
04	/HOLD/	BEN. WILL CALL, PAY UPON IDENT. ZAHLET NUR NACH IDENTIFIKATION
06	/PHON/	TELEPHONE ADVICE ACC. WITH-BANK TELEFONAVISIERET BANK D. BEGÜNSTIGTEN
07	/TELE/	TELECOMM. ADVICE ACC. WITH-BANK TELEAVISIERET BANK D. BEGÜNSTIGTEN
09	/PHONBEN/	TELEPHONE ADVICE TO BENEFICIARY TELEFONAVISIERET BEGÜNSTIGTEN
10	/TELEBEN/	TELECOMM. ADVICE TO BENEFICIARY TELEAVISIERET BEGÜNSTIGTEN
11	/CORPTRAD/	TRADE-SETTL., E.G. FX- OR SECUR.-DEAL DECKUNG, Z.B. DEISEN- O. WP-GESCH.
12	/INTRACOM/	INTRA-COMPANY PAYMENT KONZERNINTERNE ZAHLUNG
90		DM-Gegenwertzahlung: (Verwendung ist nur in Feld T19 zugelassen, siehe Anhang 1a)
91		Euro-Gegenwertzahlung: (Verwendung ist nur in Feld T19 zugelassen, siehe Anhang 1a)
95		Beträge in den Datensätzen U, V, W: in Auftragswährung. (Verwendung ist nur in Feld T18 zugelassen, siehe Anhang 3, Abschnitt D)

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 113

◆ Anhang 3: Erläuterungen der Deutschen Bundesbank zu beleglos erteilten Zahlungsaufträgen im Außenwirtschaftsverkehr

Zu Zahlungsaufträgen im Außenwirtschaftsverkehr sind statistische Angaben nach §§ 59 ff. AWV abzugeben. Die statistischen Angaben, für die eine gesetzliche Auskunftspflicht besteht, sind zur Erstellung der deutschen Zahlungsbilanz durch die Bundesbank erforderlich. Diese Angaben unterliegen der Geheimhaltung und werden nicht an andere Stellen weitergegeben.

Rechtsgrundlagen: Außenwirtschaftsgesetz (AWG), Außenwirtschaftsverordnung (AWV), Bundesstatistikgesetz (BStatG).

A. Meldepflicht und Meldefreigrenze

1. Zu melden sind Zahlungen von Gebietsansässigen über gebietsansässige Geldinstitute:

- an Gebietsfremde auf Auslandskonten;
- an Gebietsfremde auf Inlandskonten;
- für Rechnung von Gebietsfremden an Gebietsansässige;
- auf eigene Konten oder auf Konten anderer Gebietsansässiger im Ausland, soweit die vereinbarte Einlagedauer mehr als 12 Monate beträgt.

2. Nicht zu melden sind:

- Zahlungen bis zum Betrage von 5.000 DM oder Gegenwert;
- Auszahlungen oder Rückzahlungen von Krediten und Einlagen mit einer vereinbarten Laufzeit bis zu 12 Monaten;
- Zahlungen zwischen Gebietsfremden und deren Weiterleitung durch Gebietsansässige.

B. Abgabe der Meldung (Feld 9 des Datensatzes Q)

Bei meldepflichtigen Zahlungen sind grundsätzlich sowohl bei Datenträgeraustausch als auch bei Datenfernübertragung die Datensätze U und/oder W zu belegen und zusammen mit dem Zahlungsauftrag (Datensätze Q und T) beim beauftragten Geldinstitut einzureichen. Zahlungen im Transithandel sollen gesammelt mit Vordruck Z4 bzw. mit entsprechenden Datensätzen gemeldet werden. Sie können auch einzeln mit dem Datensatz V in diesem Datenträgeraustausch oder dieser Datenfernübertragung gemeldet werden.

Meldung in anderer Form:

<u>Sachverhalt</u>	<u>AWV-Vordruck</u>
Transithandel	Z4 (vorzugsweise)
Ausnahmegenehmigungen	Z4 (wie vereinbart)
Ausgleich von Salden aus Verrechnungskonten	Z4 (Meldung von Bruttozahlungen obligatorisch)
Zahlungen im Zusammenhang mit dem Betrieb der Seeschifffahrt	Z8 (obligatorisch)

Das Feld 9 des Datensatzes Q muß mit 'J' belegt werden, wenn die Datei mindestens einen Meldedatensatz (U, V oder W) enthält.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 114	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

C. Angaben zum Zahlungspflichtigen (Feld 24 des Datensatzes T)

Falls der im Datensatz Q genannte Auftraggeber Zahlungen für Dritte (z.B. Konzerntöchter) in Auftrag gibt, sind im Feld 24 des Datensatzes T das Kennzeichen 'INVF', die Bundesland-Nummer und die Firmennummer bzw. Bankleitzahl des Zahlungspflichtigen einzufügen.

D. Meldewährung (Feld 18 des Datensatzes T)

Ab Beginn der 3. Stufe der Europäischen Währungsunion können die Beträge in den Meldedatensätzen U, V und W wahlweise in DM oder der in Feld T13 genannten Auftragswährung angegeben werden. Die Verwendung der Auftragswährung anstelle DM ist mit '95' im Feld T18 zu kennzeichnen.

E. Erläuterungen zu einzelnen Positionen

Transithandel (Datensatz V) siehe B.

Sonstige Zahlungen (beispielsweise für Dienstleistungen und im Kapitalverkehr) (Datensatz W)

Die der Zahlung zugrundeliegenden Leistungen sind in Feld 10 des Datensatzes W möglichst präzise und unmißverständlich zu beschreiben, bei Wertpapiergeschäften sind die Wertpapierbezeichnungen anzugeben.

Kennzahl (Feld 4 des Datensatzes W)

Für die Kennzahl gilt das Leistungsverzeichnis (Anlage LV zur AWV, erhältlich bei Ihrer Landeszentralbank).

Falls Sie keine zutreffende Kennzahl (Leistungsart) finden, setzen Sie bitte die Sammelkennzahl 900 ein und beschreiben Sie ausführlich die zugrundeliegende Leistung im Feld 10.

Land (Felder 5 und 6 des Datensatzes W)

In der Regel ist hier anzugeben:

Land, in dem der Gläubiger der Zahlung ansässig ist;

davon abweichend gilt:

- bei ausländischen Wertpapieren: Land des Emittenten
- bei ausländischen Finanzderivaten: Land des Börsensitzes bzw. des Stillhalters
- bei Darlehensauszahlung und beim Ankauf von Auslandsforderungen: Land des Schuldners
- bei Direktinvestitionen im Ausland: Land, in dem sich das Investitionsobjekt befindet
- bei Grundstücken im Ausland: Land, in dem sich das Grundstück befindet
- bei Zahlungen für Baustellen im Land der Baustelle

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 115

Ausland:

- bei unentgeltlichen Zuwendungen Land des Begünstigten (Schenkungen):

Gegebenenfalls ist anstelle des Landes der Name der Internationalen Organisation in Abkürzung einzusetzen.

F. Auskünfte

Auskünfte und Informationsmaterial, z. B. Erläuterungen zum Leistungsverzeichnis, erhalten Sie bei der für Sie zuständigen Landeszentralbank. ☎ 0130-123411 (gebührenfrei)

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 116	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

LÄNDERVERZEICHNIS FÜR DIE ZAHLUNGSBILANZSTATISTIK DER BUNDESREPUBLIK DEUTSCHLAND

mit den gebräuchlichen Abkürzungen und dem ISO-Währungscode 1)

(Zahlungen von/an Internationale(n) Organisationen, siehe Fußnote 2)

Quelle: DEUTSCHE BUNDESBANK

Stand: Januar 1997

<i>Länderschlüssel - Land</i>	<i>Länder- abkür- zungen</i>	<i>ISO- Währungs- code</i>	<i>Länderschlüssel - Land</i>	<i>Länder- abkür- zungen</i>	<i>ISO- Währungs- code</i>
647 Abu Dhabi	A Emir	AED	413 Bermuda	Bermud	BMD
653 Aden	Jemen	YER	675 Bhutan	* Bhutan	BTN/INR
647 Adschman	A Emir	AED	676 Birma (ehem.)	Myan	MMK
220 Ägypten	Aegypt	EGP	516 Bolivien	Boliv	BOB
310 Äquatorialguinea	Ae Gui	XAF	478 Bonaire	NL Ant	ANG
334 Äthiopien	Aethio	ETB	701 Borneo, Nord-	Malays	MYR
660 Afghanistan	Afghan	AFA	700 Borneo, Süd-	Indone	IDR
070 Albanien	Alban	ALL	093 Bosnien-Herzegowina	* B Herz	BAD
208 Algerien	Alger	DZD	391 Botsuana	Botsu	BWP
811 Alofi-Insel	Wallis	XPF	508 Brasilien	Brasil	BRL
457 Amerik. Jungfernins.	Am Jgf	USD	357 Brit. Gebiet im	Ind Oz	GBP
810 Amerik.-Ozeanien	Am Oz	USD	Indischen Ozean		
810 Amerik.-Samoa	Am Oz	USD	468 Brit. Jungferninseln	* Br Jgf	USD
355 Amiranteninseln	* Seych	SCR	703 Brunei	Brunei	BND
043 Andorra	* Andorr	ESP/FRF	039 Büsingen	Schwz	CHF
330 Angola	* Angola	AOR	068 Bulgarien	Bulgar	BGL
446 Anguilla	Anguil	XCD	094 Bundesrepublik Jugo-	* Br Jug	YUM
310 Annobon-Insel	Ae Gui	XAF	slawien		
890 Antarktis	Polar	FRF	236 Burkina Faso	Burkin	XOF
459 Antigua	Antigu	XCD	328 Burundi	Burund	BIF
478 Antillen, Niederl.	NL Ant	ANG			
647 Arab. Emirate, Ver.	A Emir	AED	330 Cabinda-Landana	* Angola	AOR
528 Argentinien	Argent	ARS	454 Caicosinseln	Turk I	USD
077 Armenien	Armen	AMD	804 Campell-Insel	Neusee	NZD
474 Aruba	Aruba	AWG	022 Ceuta	Ceuta	ESP
329 Ascension	St Hel	SHP	669 Ceylon (ehem.)	Srilan	LKR
078 Aserbaidsschan	Aserb	AZM	512 Chile	Chile	CLP
800 Australien	Austrl	AUD	720 China	China	CNY
802 Austral.-Ozeanien	Aus Oz	AUD	814 Cookinseln	Neu Oz	NZD
625 Autonomiegebiet	* Wj Gaz	.	436 Costa Rica	Costa	CRC
(ehem.)			272 Côte d'Ivoire	Elfbk	XOF
010 Azoren	Portug	PTE	442 Cristobal	Panama	PAB
			478 Curacao-Insel	NL Ant	ANG
453 Bahamas	Bahama	BSD			
640 Bahrain	Bahrai	BHD	008 Dänemark	Daenm	DKK
810 Baker	Am Oz	USD	284 Dahome (ehem.)	Benin	XOF
666 Bangladesch	Bangla	BDT	001 Désirade-Insel	* Frankr	FRF
469 Barbados	Barbad	BBD	460 Dominica	Domini	XCD
459 Barbuda	Antigu	XCD	456 Dominik. Rep.	Dom Rp	DOP
073 Belarus	W Russ	BYB	338 Dschibuti	Dsbuti	DJF
825 Belau (ehem.)	* Palau	USD	647 Dubai	A Emir	AED
102 Belgien3)	Belgie	BEF			
421 Belize	Belize	BZD	500 Ecuador	Ecuad	ECS
284 Benin	Benin	XOF	272 Elfenbeinküste	Elfbk	XOF

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 117

<i>Länderschlüssel - Land</i>	<i>Länder- abkür- zungen</i>	<i>ISO- Währungs- code</i>	<i>Länderschlüssel - Land</i>	<i>Länder- abkür- zungen</i>	<i>ISO- Währungs- code</i>
428 El Salvador	El Sal	SVC	612 Irak	Irak	IQD
336 Eritrea	Eritre	ETB	616 Iran	Iran	IRR
053 Estland	Estld	EEK	007 Irland	Irland	IEP
			024 Island	Island	ISK
041 Färöer	Faroer	DKK	624 Israel	Israel	ILS
529 Falklandinseln	Falkl	FKP	005 Italien	Ital	ITL
815 Fidschi	Fidsch	FJD			
032 Finnland	Finnl	FIM	464 Jamaika	Jamaik	JMD
823 Föderierte Staaten von Mikronesien	Mikron	USD	732 Japan	Japan	JPY
736 Formosa	Taiwan	TWD	653 Jemen	Jemen	YER
001 Frankreich	Frankr	FRF	625 Jericho (ehem.)	* Wj Gaz	.
001 Franz.-Guayana	* Frankr	FRF	628 Jordanien	Jordan	JOD
822 Franz.-Polynesien	F Poly	XPF	094 Jugoslawien,Bundesre- publik	* Br Jug	YUM
647 Fudschaira	A Emir	AED	457 Jungferninseln, Amerik.	Am Jgf	USD
811 Futuna	Wallis	XPF	468 Jungferninseln, Brit.	* Br Jgf	USD
314 Gabun	Gabun	XAF	463 Kaimaninseln	Kaiman	KYD
500 Galapagos-Inseln	Ecuad	ECS	696 Kambodscha	Kambod	KHR
252 Gambia	Gambia	GMD	302 Kamerun	Kameru	XAF
625 Gaza (ehem.)	* Wj Gaz	.	404 Kanada	Kanada	CAD
625 Gazastreifen/West- jordanland	* Wj Gaz	.	006 Kanalinseln, Brit.	G Brit	GBP
076 Georgien	* Georg	GEL	011 Kanarische Inseln	* Span	ESP
822 Gesellschafts-Inseln	F Poly	XPF	247 Kap Verde	K Verd	CVE
276 Ghana	Ghana	GHC	823 Karolinen-Inseln	Mikron	USD
044 Gibraltar	Gibral	GIP	079 Kasachstan	Kasach	KZT
812 Gilbert-Inseln (ehem.)	Kiriba	AUD	644 Katar	Katar	QAR
329 Gough	St Hel	SHP	346 Kenia	Kenia	KES
473 Grenada	Grenad	XCD	083 Kirgisistan	Kirgis	KGS
009 Griechenland	Griech	GRD	812 Kiribati	Kiriba	AUD
406 Grönland	Groenl	DKK	802 Kokosinseln	Aus Oz	AUD
006 Großbritannien	G Brit	GBP	480 Kolumbien	Kolumb	COP
001 Guadeloupe	* Frankr	FRF	375 Komoren	Komor	KMF
810 Guam	Am Oz	USD	318 Kongo	Kongo	XAF
416 Guatemala	Guatem	GTQ	092 Kroatien	* Kroat	HRK
001 Guayana, Franz.-	* Frankr	FRF	448 Kuba	Kuba	CUP
310 Guinea, Äquatorial-	Ae Gui	XAF	636 Kuwait	Kuwait	KWD
257 Guinea-Bissau	Bissau	GWP			
260 Guinea	Guinea	GNF	701 Labuan	Malays	MYR
488 Guyana	Guyana	GYD	684 Laos	Laos	LAK
			395 Lesotho	* Lesoth	LSL/ZAR
452 Haiti	* Haiti	HTG	001 Les Saintes-Inseln	* Frankr	FRF
802 Heard-Insel	Aus Oz	AUD	054 Lettland	Lettld	LVL
424 Honduras	Hondur	HNL	604 Libanon	Liban	LBP
740 Hongkong	Hongk	HKD	268 Liberia	Liberi	LRD
810 Howland-Insel	Am Oz	USD	216 Libyen	Libyen	LYD
			037 Liechtenstein	Liecht	CHF
664 Indien	Indien	INR	055 Litauen	Litau	LTL
700 Indonesien	Indone	IDR	800 Lord-Howe-Insel (austral.)	Austrl	AUD
720 Innere Mongolei	China	CNY	806 Lord-Howe-Insel (Salomonen)	Salom	SBD
- Internationale Organisationen 2)			104 Luxemburg 3)	Luxbg	LUF

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 118	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

<i>Länderschlüssel - Land</i>	<i>Länder- abkür- zungen</i>	<i>ISO- Währungs- code</i>	<i>Länderschlüssel - Land</i>	<i>Länder- abkür- zungen</i>	<i>ISO- Währungs- code</i>
743 Macau	Macau	MOP	236 Obervolta (ehem.)	Burkin	XOF
370 Madagaskar	Madag	MGF	038 Österreich	Oester	ATS
010 Madeira	Portug	PTE	649 Oman	Oman	OMR
386 Malawi	Malawi	MWK	701 Ostmalaysia	Malays	MYR
701 Malaysia	Malays	MYR	810 Ozeanien, Amerik.	Am Oz	USD
667 Malediven	Maldiv	MVR	802 Ozeanien, Austral.	Aus Oz	AUD
232 Mali	Mali	XOF	814 Ozeanien, Neuseel.	Neu Oz	NZD
046 Malta	Malta	MTL			
006 Man, Insel	G Brit	GBP	662 Pakistan	Pakist	PKR
720 Mandschurei	China	CNY	825 Palau	* Palau	USD
001 Marie-Galante-Insel	* Frankr	FRF	442 Panama	* Panama	PAB/USD
204 Marokko	Marokk	MAD	(einschl. Kanal-Zone)		
824 Marshall-Inseln	Marsh	USD	801 Papua-Neuguinea	Papua	PGK
001 Martinique	* Frankr	FRF	520 Paraguay	Paragu	PYG
228 Mauretanien	Mauret	MRO	810 Pazifische Inseln	Am Oz	USD
373 Mauritius	Maurit	MUR	504 Peru	Peru	PEN
377 Mayotte	Mayott	FRF	708 Philippinen	Philip	PHP
096 Mazedonien, ehem. jugosl. Republik	Mazed	MKD	813 Pitcairn	Pitcai	NZD
802 McDonald-Inseln	Aus Oz	AUD	890 Polargebiete	Polar	FRF
022 Melilla	Ceuta	ESP	060 Polen	* Polen	PLN
412 Mexiko	Mexiko	MXN	822 Polynesien, Franz.	F Poly	XPF
810 Midway-Inseln	Am Oz	USD	010 Portugal	Portug	PTE
823 Mikronesien	Mikron	USD	311 Principe	S Tome	STD
408 Miquelon	Pierre	FRF	400 Puerto Rico	USA	USD
074 Moldau	Moldau	MDL			
001 Monaco	Frankr	FRF	647 Ras al-Chaima	A Emir	AED
716 Mongolei	Mongol	MNT	001 Réunion	* Frankr	FRF
094 Montenegro (ehem.)	* Br Jug	YUM	382 Rhodesien (ehem.)	Simbab	ZWD
470 Montserrat	Monts	XCD	732 Riukiu-Inseln	Japan	JPY
366 Mosambik	Mosamb	MZM	324 Ruanda	Ruanda	RWF
676 Myanmar	Myan	MMK	066 Rumänien	Rumaen	ROL
			075 Rußland	Russld	RUR
389 Namibia	* Namib	NAD/ZAR	478 Saba	NL Ant	ANG
803 Nauru	Nauru	AUD	701 Sabah	Malays	MYR
672 Nepal	Nepal	NPR	801 Salomon-Inseln	Papua	PGK
809 Neukaledonien	Neukal	XPF	806 Salomonen	Salom	SBD
814 Neuseel. Ozeanien	Neu Oz	NZD	378 Sambia	Sambia	ZMK
804 Neuseeland	Neusee	NZD	810 Samoa, Amerik.	Am Oz	USD
449 Nevis	St Chr	XCD	819 Samoa, West-	WSamoa	WST
432 Nicaragua	Nicara	NIO	047 San Marino	Marino	ITL
478 Niederl. Antillen	NL Ant	ANG	352 Sansibar	Tansan	TZS
003 Niederlande	Niedl	NLG	806 Santa-Cruz-Inseln	Salom	SBD
240 Niger	Niger	XOF	311 São Tomé	S Tome	STD
288 Nigeria	Nigeri	NGN	701 Sarawak	Malays	MYR
814 Niue-Inseln	Neu Oz	NZD	632 Saudi-Arabien	Saudia	SAR
820 Nördliche Marianen	Marian	USD	647 Scharidscha	A Emir	AED
701 Nordborneo (Sabah)	Malays	MYR	030 Schweden	Schwed	SEK
006 Nordirland	G Brit	GBP	039 Schweiz	Schwz	CHF
724 Nordkorea	N Korea	KPW	248 Senegal	Seneg	XOF
802 Norfolkinseln	Aus Oz	AUD	094 Serbien (ehem.)	* Br Jug	YUM
028 Norwegen	Norweg	NOK	355 Seychellen	* Seych	SCR

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 119

<i>Länderschlüssel - Land</i>	<i>Länder- abkür- zungen</i>	<i>ISO- Währungs- code</i>	<i>Länderschlüssel - Land</i>	<i>Länder- abkür- zungen</i>	<i>ISO- Währungs- code</i>
680 Siam	Thail	THB	244 Tschad	Tschad	XAF
264 Sierra Leone	Sier L	SLL	357 Tschagos-Inseln	Ind Oz	GBP
664 Sikkim	Indien	INR	061 Tschech. Republik	Tsche	CZK
382 Simbabwe	Simbab	ZWD	822 Tuamotu-Inseln	F Poly	XPF
706 Singapur	Singap	SGD	822 Tubuai-Inseln	F Poly	XPF
063 Slowakei	Slowak	SKK	052 Türkei	Tuerk	TRL
091 Slowenien	Slowen	SIT	212 Tunesien	Tunes	TND
342 Somalia	Somali	SOS	080 Turkmenistan	Turkm	TMM
822 Sous-le-Vent-Inseln	F Poly	XPF	454 Turksinseln	Turk I	USD
011 Spanien	Span	ESP	807 Tuvalu	Tuvalu	AUD
028 Spitzbergen	* Norweg	NOK			
669 Sri Lanka	Srilan	LKR	350 Uganda	Uganda	UGX
001 St. Barthélemy-Insel	* Frankr	FRF	072 Ukraine	Ukrain	UAH
449 St. Christoph (St. Kitts)-Nevis	St Chr	XCD	647 Umm al-Kaiwain	A Emir	AED
478 St. Eustatius	NL Ant	ANG	064 Ungarn	Ungarn	HUF
329 St. Helena	St Hel	SHP	524 Uruguay	Urugu	UYU
449 St. Kitts	St Chr	XCD	081 Usbekistan	Usbek	UZS
465 St. Lucia	Lucia	XCD			
001 St. Martin (franz.)	* Frankr	FRF	816 Vanuatu	Vanua	VUV
478 St. Martin (niederl.)	NL Ant	ANG	045 Vatikanstadt	Vatik	ITL
408 St. Pierre	Pierre	FRF	484 Venezuela	Venezu	VEB
467 St. Vincent	Vincen	XCD	647 Ver. Arabische Emirate	A Emir	AED
224 Sudan	* Sudan	SDD/SDP	400 Ver. Staaten von Amerika	USA	USD
388 Südafrika	S Afr	ZAR	006 Vereinigtes Königreich	G Brit	GBP
700 Südborneo	Indone	IDR	690 Vietnam	Vietn	VND
890 Südgeorgien	Polar	FRF			
728 Südkorea	S Korea	KRW	810 Wake-Insel	Am Oz	USD
890 Süd-Sandwich-Inseln	Polar	FRF	811 Wallis	Wallis	XPF
492 Suriname	Surin	SRG	802 Weihnachtsinseln	Aus Oz	AUD
028 Svalbard	* Norweg	NOK	(Ind. Ozean)		
424 Swan-Inseln	Hondur	HNL	812 Weihnachtsinseln	Kiriba	AUD
393 Swasiland	Swasi	SZL	(Paz. Ozean)		
608 Syrien	Syrien	SYP	073 Weißrußland	W Russ	BYB
			625 Westjordanland/Gaza- streifen	* Wj Gaz	.
082 Tadschikistan	* Tadsch	TJR	819 Westsamoa	Wsamoa	WST
822 Tahiti-Insel	F Poly	XPF			
736 Taiwan	Taiwan	TWD	322 Zaire	Zaire	ZRN
352 Tansania	Tansan	TZS	306 Zentralafrik. Republik	Zentaf	XAF
800 Tasmanien	Austrl	AUD	600 Zypern	Zypern	CYP
011 Teneriffa	* Span	ESP			
680 Thailand	Thail	THB	- Internationale Organi- sationen (vgl. Fußnote)		
720 Tibet	China	CNY	nachrichtlich:		
472 Tobago	Trinid	TTD			
280 Togo	Togo	XOF			
814 Tokelau-Inseln	Neu Oz	NZD	- Europäische Währungseinheit		XEU
817 Tonga	Tonga	TOP			
472 Trinidad	Trinid	TTD			
329 Tristan da Cunha	St Hel	SHP			

1) Basierend auf dem Länderverzeichnis für die Außenhandelsstatistik der Bundesrepublik Deutschland (Statistisches Bundesamt). - Zur Zuordnung einzelner Gebiete zu bestimmten Ländern siehe: "Regional-

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 120	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

systematik - Alphabetisches Länderverzeichnis für die Außenhandelsstatistik", hrsg. vom Statistischen Bundesamt.

- 2) Eingehende und ausgehende Zahlungen von/an Internationale(n) Organisationen sollen in den Meldungen unter ihrem Namen und nicht unter dem jeweiligen Land ausgewiesen werden (siehe BBk-Mitteilung Nr. 8003/93).**
- 3) Abweichende Länder-Nummern vom Länderverzeichnis für die Außenhandelsstatistik.**

Das Länderverzeichnis dient nur statistischen Zwecken. Aus den Bezeichnungen kann keine Bestätigung oder Anerkennung des politischen Status eines Landes oder der Grenzen seines Gebietes abgeleitet werden.

- * Veränderungen der letzten beiden Jahre gegenüber dem Länderverzeichnis (Stand: Januar 1995) sind mit * gekennzeichnet.**

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 121

VIII.9.3 SWIFT-Formate

Trennzeichen gemäß SWIFT-User-Handbook:

- Vor jeder Feldnummer:
 - CRLF bei DFÜ (ASCII: X'0D0A', EBCDIC: X'0D25')
 - C'@@ bei Btx
- Eine Nachricht bzw. Teilnachricht wird mit X'0D0A2D' (ASCII) bzw. X'0D2560' (EBCDIC) abgeschlossen. Bei Btx nur C'@@'.

SWIFT-Zeichensatz:

a b c d e f g h i j k l m n o p q r s t u v w x y z

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0 1 2 3 4 5 6 7 8 9

/ = ? : () . , ' + { }

CR LF Space

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 122	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

VIII.9.3.1 MT 571

Nr.	Name	Format ¹	Länge	Status	Bemerkungen
:28:	SEITENANZAHL Subfeld 1: Lfd. Nummer Subfeld 2: Endekennzeichen	9 9	..5 3	M M	Der Feldinhalt wird pro SWIFT-Message hochgezählt Bei der letzten SWIFT-Message wird „/99“ hinterlegt, bei allen anderen „/00“.
:20:	REFERENZNUMMER	X	..16	M	xxxxxxxx/yyyyyy oder xxxxxxxxxxxx/yyyy x = BLZ oder SWIFT-Adresse y = 7- oder 4-stellige Nummer
:21:	KUNDENREFERENZ	X	..16	M	Kunden-Referenznummer oder NONREF
:83a:	DEPOT Variante A: Subfeld 1: Depotnummer Subfeld 2: Adresse	X X	..37 ..11	M M	Diese Variante soll nicht genutzt werden /C/xxx...xx oder /D/xxx...xx C = Credit (Vorzeichen) D = Debit (Vorzeichen) x = Depotnummer (max. 34 Stellen) SWIFT-Adresse (BIC-Code)
	Variante C: Depotnummer	X	..35	M	/xxxxxxxx/yyy...yy oder xxxxxxxxxxxx/yyy...yy x = BLZ oder SWIFT-Adresse y = Depotnummer
	Variante D: Subfeld 1: Depotnummer	X	..37	M	Diese Variante soll nicht genutzt werden. /C/xxx...xx oder /D/xxx...xx C = Credit (Vorzeichen) D = Debit (Vorzeichen) x = Depotnummer (max. 34 Stellen)
:67A:	AUFSTELLUNGS- STICHTAG	9	6	M	JJMMTT
:30:	ERSTELLUNGSDATUM	9	6	K	JJMMTT

Die Felder :35H: bis :72: können in Abweichung zur SWIFT-Blockbegrenzung beliebig oft wiederholt werden.

¹ X = alphanumerisch, 9 = numerisch

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 123

↓ Beginn des Wiederholungszyklus gemäß S.W.I.F.T.

Nr.	Name	Format	Länge	Status	Bemerkungen
:35H:	ANZAHL				
	Subfeld 1: Negativer Bestand	X	1	K	fest belegt mit „N“ bei negativem Bestand
	Subfeld 2: Währung	X	3	K	ISO-Code der Währung oder Codeworte: BON: Bonds - in Stück notierte Anleihen (Stück) FMT: Face or principal on promised amount-Anleihen mit Prozentnotiz MSC: Miscellaneous - Sonstige Empfehlung (Benutzung sollte vermieden werden, da nicht eindeutig identifizierbar) OPC: Option contracts - Optionskontrakte (Kontrakte) RTS: Rights - Bezugsrechte (Stück) SHS: Shares - Anteilsscheine (Stück) UNT: Units (e.g., consists of a bond and a warrant) - Anteile (Stück) WTS: Warrants - Optionsscheine (Stück)
	Subfeld 3: Anzahl	9	..15	K	Anzahl nominal oder Stück
:35B:	WP-KENNUMMER und -BEZEICHNUNG				
	Subfeld 1: WP-Kennnummer	X	17	K	ISIN_XXYYYYYYYYYP Nur sofern die ISIN-Kennnummer nicht existiert, wird hinterlegt: WKNR_ZZZZZZ _ = Leerzeichen X = ISO-Ländercode Y = internationale WP-Kennnummer P = Prüfbyte Z = deutsche Wertpapierkennnummer
	Subfeld 2: WP-Bezeichnung	X	4 x ..35	K	
:33B:	KURS				
	Subfeld 1: Währung	X	3	K	ISO-Währungscode oder Codeworte: PCT: Percentage Price REN: Revenue Amount YLD: Yield Price
	Subfeld 2: Betrag	9	..15	K	Betrag, Dezimalstellen sind durch ein Komma abzutrennen
:34a:	STÜCKZINSEN				
	Variante G (positive Stückzinsen):				

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 124	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

Nr.	Name	Format	Länge	Status	Bemerkungen
	Subfeld 1: Zinstage	9	3	K	Anzahl der Tage, rechtsbündig einstellen, alle drei Stellen müssen belegt werden, evtl. mit Nullen auffüllen.
	Subfeld 2: Währung	X	3	K	ISO-Code der Währung. Wenn Feld :34a: belegt ist, muß auch der ISO-Code eingetragen sein.
	Subfeld 3: Betrag	9	..15	K	Aufgelaufener positiver Stückzinsbetrag. Wenn Feld :34a: belegt ist, muß auch der Betrag eingetragen sein.
	Variante H (negative Stückzinsen):				
	Subfeld 1: Zinstage	9	3	K	Anzahl der Tage, rechtsbündig einstellen, alle drei Stellen müssen belegt werden, evtl. mit Nullen auffüllen.
	Subfeld 2: Währung	X	3	K	ISO-Code der Währung. Wenn Feld :34a: belegt ist, muß auch der ISO-Code eingetragen sein.
	Subfeld 3: Betrag	9	..15	K	Aufgelaufener positiver Stückzinsbetrag. Wenn Feld :34a: belegt ist, muß auch der Betrag eingetragen sein.
:36:	DEISENKURS	9	..12	K	Umrechnungskurs :33B: zu :32H:
:32H:	KURSWERT				Kurswert der Position
	Subfeld 1: Kennzeichnung eines Negativbetrags	X	1	K	Wenn es sich um einen negativen Betrag handelt, ist „N“ einzustellen.
	Subfeld 2: Währung	X	3	K	ISO-Code der Währung
	Subfeld 3: Betrag	9	..15	K	Betrag, Dezimalstellen sind durch ein Komma abzutrennen
:72:	ZUSATZINFORMATIONEN	X	6 x ..35	K	Codeworte gemäß SWIFT: BLOCKED BORROWED COLLATER DISCOUNT LOANDOUT NOHOLDGS PREMIUM REGOPEN VALUDATE zusätzlich strukturierte Belegung s. Anlage, beginnend in Zeile 2

↑ Ende des Wiederholungszyklus gemäß S.W.I.F.T.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 125

Nr.	Name	Format	Länge	Status	Bemerkungen
:18A:	ANZAHL VON WIEDERHOLUNGSZYKLEN	9	..5	M	Der Inhalt dieses Feldes ist gleich der Anzahl der Depotpositionen, die in der Nachricht aufgelistet werden.
:34E:	DEPOTWERT (N) Subfeld 1: Kennzeichnung eines negativen Depotwerts Subfeld 2: Währung Subfeld 3: Betrag	X X 9	1 3 ..15	K M M	Wenn es sich um einen negativen Betrag handelt, ist hier „N“ einzustellen. ISO-Code der Währung Betrag, Dezimalstellen sind durch ein Komma abzutrennen
:72:	ZUSATZINFORMATIONEN	X	6 x ..35	K	Codeworte gemäß SWIFT: BLOCKED BORROWED COLLATER DISCOUNT LOANDOUT NOHOLDGS PREMIUM REGOPEN VALUDATE zusätzlich strukturierte Belegung s. Anlage, beginnend in Zeile 2

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 126	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

♦ **Strukturierte Belegung des Feldes :72: für die S.W.I.F.T.-Datenformate MT5xx, beginnend in Zeile 2**

Name	Feld-schlüssel ²	For-mat	Län-ge	Sta-tus	Bemerkungen
Depotwährung		X	3	K	Folgende Codeworte sind möglich: STK: Stück-notierte Wertpapiere KON: Kontrakte ISO-Währungscode der Gattungswährung - prozentnotierte Wertpapiere
Wertpapierart	00	9	3	K	gemäß WM GD 195
Abrechnungsart	01	9	1	K	fest belegt mit '1' = Netto
Lagerland	02	X	2	K	ISO-Code
Verwahrart	03	9	2	K	gemäß WM GD 400
Branchenschlüssel	04	9	5	K	gemäß WM GD 200
Länderschlüssel (Land des Emittenten)	05	X	2	K	ISO-Code
Emittentenschlüssel	06	9	8	K	gemäß WM GD 205
Sperre bis	07	9	6	K	JJMMTT
Sperrvermerke/Zusatzvermerke der Bank	08	X	³⁾	K	
Zusatzangaben/Buchungstext	09	X	⁴⁾	K	
Fälligkeitsdatum	10	9	6	K	JJMMTT

♦ **Ergänzende Festlegung zu den einzelnen Feldschlüsseln:**

- Das Feld „Zusatzangaben/Buchungstext“ teilt sich die Feldlänge mit dem Feld „Sperrvermerke“. Die Belegung orientiert sich an dem Aufbau der DTB-Datensätze.
- Für die Belegung des Feldes „Zusatzangaben/Buchungstext“ gilt folgende Spezifikation:

Nr.	Subfeld	Län-ge	Inhalt
1	Symbol	4	Kürzel z.B. „FDAX“ oder „BMW“ (ggf. Blanks)
2	Schlüssel	1	C = Call, P = Put, F = Future
3	Verfall-Datum	4	JJMM
4	Basispreis Subfeld 1 Subfeld 2	3 .. 15	ISO-Währungscode Betrag
5	Version	1	z.B. 0/1/2/3

² Vor jedem **Feldschlüssel** ist als Trennzeichen ein „/“ anzugeben.

³ max. 110 Stellen abzüglich der von Feldschlüssel „09“ belegten Stellenzahl

⁴ max. 110 Stellen abzüglich der von Feldschlüssel „08“ belegten Stellenzahl

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 127

Nr.	Subfeld	Länge	Inhalt
6	Unit	8	Kontraktgröße
7	WKN des Underlying	..	6 Zeichen bei deutscher WKN 17 Zeichen bei ISIN Nr. beginnend mit ISIN

♦ **Beispiel zur strukturierten Belegung des Feldes :72:**

```
:72:/AGEN/@@
STR?00511?011?02DE?0303@@
0400081?05DE?0620030020?07900228@@
08Verpfändet für Darlehen Nr. 60200@@
```

@@ = CRLF (SWIFT-Trennzeichen)

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 128	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

VIII.9.3.2 MT 940

Nr.	Name	Format ⁶	Länge	Status	Bemerkungen
:20:	Auftragsreferenznummer	X	..16	M	nicht strukturiert
:21:	Bezugsreferenznummer	X	..16	K	wird nicht ausgegeben
:25:	Kontobezeichnung	X	..35	M	xxxxxxxxxx/Kto-Nr. oder yyyyyyyy/Kto-Nr. wobei xxxxxxxxxx = SWIFT-Code yyyyyyyy = Bankleitzahl Kto-Nr. = max. 23 Stellen Kto-Nr. (ggf. mit Währung)
:28C:	Auszugsnummer ⁷	9	..9	M	Belegung: '0' oder xxxxx/yy xxxxx = Auszugsnummer yy = Blattnummer, beginnend mit 1
:60m:	Anfangssaldo		..25	M	"F" bei Anfangssaldo "M" bei Zwischensaldo (die Felder 20 - 28 müssen vor jedem Zwischen- saldo ausgegeben werden) Ausnah- men: Institutsbezogen ohne Zwi- schensaldo
	Subfeld 1: (Soll/Haben-Kennung)	X	1	M	C = Credit D = Debit
	Subfeld 2: (Buchungsdatum)	9	6	M	JJMMTT = Buchungsdatum 'ALT' oder '0' bei 1. Auszug
	Subfeld 3: (Währung)	X	3	M	Währungsschlüssel gem. ISO 4217
	Subfeld 4: (Betrag)	9	..15	M	Betrag in Kontowährung mit Komma als Dezimalzeichen (gem. SWIFT- Konventionen)
:61:	Umsatzzeile		..102	K	
	Subfeld 1 (Valuta)	9	6	M	JJMMTT
	Subfeld 2 (Buchungsdatum)	9	4	K	MMTT
	Subfeld 3 (Soll/Haben-Kennung)	X	..2	M	C = Credit D = Debit RC = Storno Credit RD = Storno Debit

⁶ X = alphanumerisch, 9 = numerisch

⁷ Bis zum 01.01.1999 kann das Kreditinstitut anstatt Feld 28C auch Feld 28 in der Form xxxxx/yy liefern.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 129

Nr.	Name	For- mat ⁶	Län- ge	Sta- tus	Bemerkungen
	Subfeld 4 (Währungsart)	X	1	K	Die dritte Stelle der Währungsbezeichnung, wenn sie zur Unterscheidung wichtig ist.
	Subfeld 5 (Betrag)	9	..15	M	Betrag in Kontowährung mit Komma als Dezimalzeichen (gem. SWIFT-Konventionen)
	Subfeld 6 (Buchungsschlüssel)	X	4	M	Codes gem. SWIFT-User-Handbuch, dabei 1. Stelle konstant "N"
	Subfeld 7 (Referenz)	X	..16	M	Kundenreferenz. Bei Nichtbelegung wird "NONREF" eingestellt (z.B. Schecknummer oder bei DTA: Feld 10 aus A-Satz)
	Trennzeichen			K	'/', wenn Subfeld 8 vorhanden
	Subfeld 8 (Bankreferenz)	X	..16	K	Bankenreferenz (z.B. bei DTA: Feld 6b)
	Trennzeichen			K	CRLF, wenn Subfeld 9 vorhanden
	Subfeld 9 ⁸ (Weitere Information/Ursprungsbetrag und Gebührenbetrag)	X	..34	M/K	Bei Abruf im Altformat: Kundenreferenz bzw. 2. Bankreferenz (Fortsetzung aus Subfeld 7) Bei Abruf im Neuformat: Währungsart und Umsatzbetrag in Ursprungswährung (original currency amount) in folgendem Format: /OCMT/3a15num/ sowie Währungsart und Gebührenbetrag (charges) in folgendem Format: /CHGS/3a15num/ 3a = 3stelliger Währungscode gemäß ISO 4217 15num = Betrag mit Komma als Dezimalzeichen (gemäß S.W.I.F.T.-Konvention)
:86:	Mehrzweckfeld		..390	K	Bei GV-Code 999: unstrukturiert max. 387 Stellen frei belegbar 6x65 Bytes getrennt durch CRLF; das letzte Subfeld wird nicht mit CRLF abgeschlossen
:62m:	Schlußsaldo		..25	M	"F" bei Schlußsaldo "M" bei Zwischensaldo
	Subfeld 1: (Soll/Haben-Kennung)	X	1	M	C = Credit D = Debit

⁸ Im Neuformat ist die Belegung des Feldes ab dem Start der Stufe 3 der EWWU empfohlen, wenn Ursprungswährung und Kontowährung voneinander abweichen. Falls die Länge nicht ausreicht, können alle Angaben auch in Feld 86 eingestellt werden. In jedem Fall sind Originalbetrag und - falls vorhanden - Gebührenbetrag in dasselbe Feld einzustellen.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 130	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

Nr.	Name	For- mat ⁶	Län- ge	Sta- tus	Bemerkungen
	Subfeld 2: (Buchungsdatum)	9	6	M	JJMMTT = aktuelles Buchungsdatum
	Subfeld 3: (Währung)	X	3	M	Währungsschlüssel gem. ISO 4217
	Subfeld 4: (Betrag)	9	..15	M	Betrag in Kontowährung mit Komma als Dezimalzeichen (gem. SWIFT-Konventionen)
:64:	Aktueller Valutensaldo		..25	K	wahlfrei; Feld 64 wird nicht in die Strukturierungsmaßnahme einbezogen.
	Subfeld 1: (Soll/Haben-Kennung)	X	1	M	
	Subfeld 2: (Buchungsdatum)	9	6	M	
	Subfeld 3: (Währung)	X	3	M	
	Subfeld 4: (Betrag)	9	..15	M	
:65:	Zukünftige Valutensalden		..25	K	wahlfrei; Feld 65 wird nicht in die Strukturierungsmaßnahme einbezogen
	Subfeld 1: (Soll/Haben-Kennung)	X	1	M	
	Subfeld 2: (Buchungsdatum)	9	6	M	
	Subfeld 3: (Währung)	X	3	M	
	Subfeld 4: (Betrag)	9	..15	M	
:86:	Mehrzweckfeld		..390	K	

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 131

◆ Anlage 2: SWIFT MT 940, Feld 86

Strukturierte Belegung des Mehrzweckfeldes⁹

Feld-schlüsse I	Name	Format	Län-ge	Sta-tus	An-zahl	Bemerkungen
	Geschäftsvorfall-Code	numerisch	3	M	1	gemäß Anlage 3
00	Buchungstext	alpha	..27	K	1	
10	Primanoten-Nr.	alphanum	..10	K	1	
20-29	Verwendungszweck ¹⁰	alphanum	..27	K	10	
30	BLZ Auftraggeber/ Zahlungsempfänger	numerisch	..12	K	1	
31	Konto-Nr. Auftraggeber/ Zahlungsempfänger	numerisch	..24	K	1	
32-33	Name Auftraggeber/ Zahlungsempfänger	alphanum	..27	K	2	
34	Textschlüsselergänzung	numerisch	3	K	1	
60-63	Verwendungszweck	alphanum	..27	K	4	

Das Steuerzeichen "?" steht vor jedem Feldschlüssel.

Beispiel:

```
86:051?00UEBERWEISUNG?100599?20XXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXX?21/E@@
CMT/DEM998,65/?3050060400?310847564700?32MUELLER
?34339@@
```

@ @ = CRLF (SWIFT-Trennzeichen)

⁹ Die strukturierte Belegung des Mehrzweckfeldes :86: ist freigestellt. Wird jedoch die strukturierte Belegung des Feldes :86: genutzt, so dürfen ausschließlich die vom ZKA in der nachfolgenden Anlage 3 definierten Geschäftsvorfall-Codes eingestellt werden.

¹⁰ Die Nutzung der Subfelder 27-29 und 60-63 ist nur im Neuformat zulässig. Soweit das Kreditinstitut im Neuformat den Umsatzbetrag auch in Äquivalenzwährung (Euro bei DM-Umsätzen und umgekehrt) mitteilt, so wird empfohlen, diesen Betrag in einem der Verwendungszweckfelder linksbündig in folgender Formatierung einzustellen:

/ECMT/3a15num/, wobei

3a = Äquivalenzwährung gemäß ISO 4217

15num = Äquivalenzbetrag mit Komma als Dezimalzeichen (gemäß S.W.I.F.T.-Konvention)

Soweit im Neuformat der Ursprungsumsatzbetrag und Gebührenbetrag nicht in Feld 61/9 eingestellt werden, so wird empfohlen, diese Angaben linksbündig in zwei aufeinanderfolgenden Verwendungszweckfeldern einzustellen.

Beispiel: ?20/OCMT/FRF1000,/?21/CHGS/EUR2,1/

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 132	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

◆ Anlage 3: Geschäftsvorfallcodes

Erläuterungen:

Der Geschäftsvorfall-Code definiert alle aus der Bankbuchung resultierenden Geschäftsvorfälle in Form eines einheitlichen dreistelligen Schlüssels, der es den Kunden ermöglicht, bei der Weiterverarbeitung von Umsatzinformationen eine Umsetzung in betriebsspezifische Geschäftsvorfallarten durchzuführen.

Aufbau des Geschäftsvorfall-Codes:

```

X  X  X
|  |  |_____Geschäftsvorfallart
|  |_____Geschäftsvorfallart
|_____Geschäftssparte

```

Stelle 1:

- 0 = Inlandszahlungsverkehr
- 1 = Inlandszahlungsverkehr
- 2 = Auslandsgeschäfts
- 3 = Wertpapiergeschäft
- 4 = Devisengeschäft
- 5 = MAOBE
- 6 = Reserve
- 7 = Reserve
- 8 = Sonstige
- 9 = Unstrukturierte Belegung

Stellen 2 und 3:

siehe nächste Seiten

Der Geschäftsvorfall-Code ist im MT 940, Feld 86, Stellen 1 bis 3 enthalten. Bei Stornobuchungen ist zusätzlich im Feld 61, Subfeld 3, die Belegung RC oder RD erforderlich.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 133

SWIFT MT 940

Zwischenbetrieblich gültige Geschäftsvorfall-Codes für Umsatzinformationen (Belegung Stellen 1 bis 3 im Mehrzweckfeld 'Feld 86')

Geschäfts- vorfall-Code	Geschäftsvorfall
0 X X	I N L A N D S Z A H L U N G S V E R K E H R
0 0 1	Inhaberscheck (nicht eurocheque)
0 0 2	Orderscheck
0 0 3	DM-Reisescheck
0 0 4	Lastschrift (Abbuchungsverfahren)
0 0 5	Lastschrift (Einzugsermächtigungsverfahren)
0 0 6	sonstige Einzugspapiere
0 0 8	Dauerauftrag Belastung
0 0 9	Retourenhülle (Lastschrift) für Einzugspapier, Rücklastschrift aus Datenträger- geraustausch, Lastschrift (Rückbelastung) - DTA -
0 1 0	Rückrechnung (Lastschrift) für - Direktrückgabe - nicht eingelösten BSE-Scheck Hülle (Lastschrift) für - angeforderten BSE-Scheck - Neueinreichung eines garantierten BSE-Schecks - Auslieferung einer BSE-Scheckkopie/eines BSE-Originalschecks Ersatzstück für verlorengegangenen Scheck
0 1 1	eurocheque
0 1 2	Zahlungsanweisung zur Verrechnung
0 1 4	Lastschrift für Fremdwährungs-eurocheque / Lastschrift für über die GZS abgewickelte Auslandsschecks
0 1 5	Auslandsüberweisung ohne Meldeteil
0 1 7	Überweisungsauftrag beim neutralen Überweisungs-/Zahlscheinvordruck mit prüfziffergesicherten Zuordnungsdaten
0 1 8	Überweisungsauftrag beim neutralen Überweisungs-/Zahlscheinvordruck
0 1 9	Überweisungsauftrag beim neutralen Spenden-Überweisungs- /Zahlscheinvordruck
0 2 0	Überweisungsauftrag
0 5 1	Überweisungsgutschrift
0 5 2	Dauerauftrags-Gutschrift
0 5 3	Lohn-, Gehalts-, Rentengutschrift
0 5 4	Vermögenswirksame Leistungen
0 5 6	Überweisung öffentlicher Kassen
0 5 8	Bank-an-Bank-Zahlung (Überweisungsgutschrift)
0 5 9	Retourenhülle (Gutschrift) für unanbringliche Überweisung, Gutschrift (Rücküberweisung) - DTA -
0 6 5	Auslandsüberweisung ohne Meldeteil
0 6 6	Gutschrift aus Scheckeinreichung E.v. (Exportscheckabwicklung über GZS)
0 6 7	Gutschrift beim neutralen Überweisungs-/Zahlscheinvordruck mit prüfziffer- gesicherten internen Zuordnungsdaten
0 6 8	Gutschrift beim neutralen Überweisungs-/Zahlscheinvordruck EZÜ
0 6 9	Gutschrift beim neutralen Spenden-Überweisungs-/Zahlscheinvordruck EZÜ
0 7 0	Scheckeinreichung
0 7 1	Lastschrifteinreichung
0 7 2	Wechseleinreichung
0 7 3	Wechsel
0 7 4	TC (Scheckbelastung)
0 7 5	Scheck BSE

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 134	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

Geschäfts- vorfall-Code Geschäftsvorfall

0 7 6	Telefonauftrag
0 7 7	BTX-Überweisung
0 7 8	Überweisung (Versorgungsbezüge)
0 7 9	Sammler
0 8 0	Gehalt
0 8 1	Vergütung
0 8 2	Einzahlungen
0 8 3	Auszahlungen
0 8 4	BTX-Einzugsauftrag
0 8 5 ¹¹	drahtlicher Überweisungsauftrag
0 8 6	drahtliche Überweisungsgutschrift
0 8 7	Überweisungsauftrag mit Festvaluta
0 8 8	Überweisungsgutschrift mit Festvaluta
0 8 9	drahtlicher Überweisungsauftrag mit Festvaluta
0 9 0	drahtliche Überweisungsgutschrift mit Festvaluta
0 9 1	DATA-Einreichung Überweisungen
0 9 2	DATA-Einreichung Lastschriften
0 9 3	Diskont-Wechsel
0 9 4	Rediskont-Wechsel
0 9 5	Aval (Inland)
0 9 6 ¹²	Kontoübertrag (Soll)
0 9 7	Kontoübertrag (Haben)
0 9 8	GeldKarte (Umsatz Elektronische Geldbörse)
0 9 9	GeldKarte (Händlerprovision für Zahlungsgarantie)

1 X X I N L A N D S Z A H L U N G S V E R K E H R Reserve

2 X X	A U S L A N D S G E S C H Ä F T
2 0 1	Zahlungsauftrag
2 0 2	Auslandsvergütung
2 0 3	Inkasso
2 0 4	Akkreditiv
2 0 5	Aval
2 0 6	Auslandsüberweisung
2 0 7	zunächst frei
2 0 8	Rembourse
2 0 9	Zahlung per Scheck
2 1 0	Zahlung über elektronische Medien
2 1 1	Zahlungseingang über elektronische Medien
2 1 2	Dauerauftrag
2 1 3	Lastschrift-Einzug aus dem Ausland
2 1 4	Dokumenten-Inkasso (Import)
2 1 5	Dokumenten-Inkasso (Export)
2 1 6	Wechsel-Inkasso (Import)
2 1 7	Wechsel-Inkasso (Export)
2 1 8	Import-Akkreditiv
2 1 9	Export-Akkreditiv
2 2 0	Gutschrift e.V. eines Auslands-Schecks
2 2 1	Gutschrift Auslands-Scheck-Inkasso
2 2 2	Belastung Auslands-Scheck

¹¹ Die Codes 085 und 086 sind nur im Altformat zulässig.

¹² Die Codes 096 bis 099 sind nur im NeufORMAT zulässig.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 135

Geschäfts- vorfall-Code	Geschäftsvorfall
----------------------------	------------------

2 2 3	Belastung Auslands-ec-Scheck
2 2 4	Sorten-Ankauf
2 2 5	Sorten-Verkauf
3 X X	W E R T P A P I E R G E S C H Ä F T
3 0 1	Inkasso
3 0 2	Kupon/Dividenden
3 0 3	Effekten
3 0 4	Übertrag
3 0 5	Namensschuldverschreibung
3 0 6	Schuldschein
3 0 7	Wertpapierzeichnung
3 0 8	Handel von Bezugsrechten
3 0 9	Handel von Bonusrechten
3 1 0	Handel von Optionen
3 1 1	Termingeschäfte
3 2 0	Gebühren für Wertpapiergeschäfte
3 2 1	Depotgebühren
3 3 0	Erträge aus Wertpapieren
3 4 0	Gutschrift für fällige Wertpapiere
3 9 9	Storno
4 X X	D E V I S E N G E S C H Ä F T
4 0 1	Kassedevisen
4 0 2	Termindevisen
4 0 3	Reisedevisen
4 0 4	Devisenscheck
4 0 5	Finanzinnovationen
4 0 6	
4 0 7	
4 0 8	
4 0 9	
4 1 0	
4 1 1	Devisenkassa-Kauf
4 1 2	Devisenkassa-Verkauf
4 1 3	Devisentermin-Kauf
4 1 4	Devisentermin-Verkauf
4 1 5	FW-Tagegeld-Aktiv
4 1 6	FW-Tagegeld-Passiv
4 1 7	FW-Termingeld-Aktiv
4 1 8	FW-Termingeld-Passiv
4 1 9	Call-Geld-Aktiv
4 2 0	Call-Geld-Passiv
4 2 1	Optionen
4 2 2	Swap
4 2 3	Edelmetall-Ankauf
4 2 4	Edelmetall-Verkauf
5 X X	M A O B E
6 X X	R E S E R V E
7 X X	R E S E R V E
8 X X	S O N S T I G E
8 0 1	Scheckkarte

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 136	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

Geschäfts- vorfall-Code	Geschäftsvorfall
----------------------------	------------------

8 0 2	Scheckheft
8 0 3	Depotverwahrung
8 0 4	Dauerauftragsgebühren
8 0 5	Abschluß
8 0 6	Porto/Zustellgebühren
8 0 7	Preise/Spesen
8 0 8	Gebühren
8 0 9	Provisionen
8 1 0	Mahngebühren
8 1 1	Kreditkosten
8 1 2	Stundungszinsen
8 1 3	Disagio
8 1 4	Zinsen
8 1 5	kapitalisierte Zinsen
8 1 6	Zinssatzänderung
8 1 7	Zinsberichtigung
8 1 8	Abbuchung
8 1 9	Bezüge
8 2 0	Übertrag
8 2 1	Telefon
8 2 2	Auszahlplan
8 2 3	Festgeld
8 2 4	Leihgeld
8 2 5	Universaldarlehn
8 2 6	dynamisches Sparen
8 2 7	Überschußsparen
8 2 8	Sparbrief
8 2 9	Sparplan
8 3 0	Bonus
8 3 1	alte Rechnung
8 3 2	Hypothek
8 3 3	Cash Concentrating - Buchung Hauptkonten
8 3 4	Cash Concentrating - Avisinformation für Nebenkonten
8 3 5	sonstige nicht definierte GV-Arten
8 3 6	Reklamationsbuchung
8 9 9	Storno
9 X X	U N S T R U K T U R I E R T E R I N H A L T
9 9 7	Depotaufstellung -> MT 571
9 9 9	Unstrukturierte Belegung des Mehrzweckfeldes Feld '86'

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 137

VIII.9.3.3 MT 942

Nr.	Name	Format ¹³	Länge	Status	Bemerkungen
:20:	Auftragsreferenznummer	X	..16	M	nicht strukturiert
:21:	Bezugsreferenznummer	X	..16	K	nicht strukturiert
:25:	Kontobezeichnung	X	..35	M	xxxxxxxxxx/Kto-Nr. oder yyyyyyyy/Kto-Nr. wobei xxxxxxxxxx = SWIFT-Code yyyyyyyy = Bankleitzahl Kto-Nr. = max. 23 Stellen Kto-Nr. (ggf. mit Währung)
:28C:	Auszugsnummer ¹⁴	9	..9	M	Belegung: '0' oder xxxxx/yyy xxxxx = Auszugsnummer yyy = Blattnummer, beginnend mit 01
:34F:	Mindestbetrag		..19	M	
	Subfeld 1: (Währung)	X	3	M	Währungsschlüssel gem. ISO-Code
	Subfeld 2: (Soll/Haben-Kennung)	X	1	M	D = Debit (Soll) C = Credit (Haben)
	Subfeld 3: (Betrag)	9	..15	M	Betrag in Kontowährung mit Komma als Dezimalzeichen (gem. SWIFT- Konventionen)
:13:	Enddatum/ Geltungs- bereich		10	M	
	Subfeld 1: Datum	9	6	M	Erstellungsdatum: JJMMTT
	Subfeld 2: Uhrzeit	9	4	M	Erstellungszeit: hhmm
:61:	Umsatzzeile		..102	K	
	Subfeld 1 (Valuta)	9	6	M	JJMMTT
	Subfeld 2 (Buchungsdatum)	9	4	K	MMTT
	Subfeld 3 (Soll/Haben-Kennung)	X	..2	M	C = Credit D = Debit RC = Storno Credit RD = Storno Debit
	Subfeld 4 (Währungsart)	X	1	K	Die dritte Stelle der Währungsbe- zeichnung, wenn sie zur Unterschei- dung wichtig ist.

¹³ X = alphanumerisch, 9 = numerisch

¹⁴ Nur im NeufORMAT zulässig.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 138	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate

Nr.	Name	Format ¹³	Länge	Status	Bemerkungen
	Subfeld 5 (Betrag)	9	..15	M	Betrag in Kontowährung mit Komma als Dezimalzeichen (gem. SWIFT-Konventionen)
	Subfeld 6 (Buchungsschlüssel)	X	4	M	Codes gem. SWIFT-User-Handbuch, dabei 1. Stelle konstant "N"
	Subfeld 7 (Referenz)	X	..16	M	Kundenreferenz. Bei Nichtbelegung wird "NONREF" eingestellt (z.B. Schecknummer oder bei DTA: Feld 10 aus A-Satz)
	Trennzeichen			K	'/', wenn Subfeld 8 vorhanden
	Subfeld 8 (Bankreferenz)	X	..16	K	Bankenreferenz (z.B. bei DTA: Feld 6b)
	Trennzeichen			K	X'0D0A' (CRLF), wenn Subfeld 9 vorhanden
	Subfeld 9 ¹⁵ (Weitere Information/ Ursprungsbetrag und Gebührenbetrag)	X	..34	K	<p>Bei Abruf im Altformat: Kundenreferenz bzw. 2. Bankreferenz (Fortsetzung aus Subfeld 7)</p> <p>Bei Abruf im Neuformat: Währungsart und Umsatzbetrag in Ursprungswährung (original currency amount) in folgendem Format: /OCMT/3a15num/ sowie Währungsart und Gebührenbetrag (charges) in folgendem Format: /CHGS/3a15num/ 3a = 3stelliger Währungscode gemäß ISO 4217 15num = Betrag mit Komma als Dezimalzeichen (gemäß S.W.I.F.T.-Konvention)</p>
:86:	Mehrzweckfeld		..390	K	Es gelten die Belegungsregeln des MT 940 einschließlich der zugehörigen Geschäftsvorfall-Codes
:90D:	Anzahl und Summe der Sollbuchungen		..23	K	Bei DFÜ-Übertragung Pflichtfeld wegen Abstimmsummen
	Subfeld 1: (Anzahl Sollbuchungen)	9	..5	M	
	Subfeld 2: (Währung)	X	3	M	Währungsschlüssel gem. ISO 4217

¹⁵ Im Neuformat ist die Belegung des Feldes ab dem Start der Stufe 3 der EWWU empfohlen, wenn Ursprungswährung und Kontowährung voneinander abweichen. Falls die Länge des Feldes nicht ausreicht, können die Angaben auch in Feld 86 eingestellt werden. In jedem Fall sind Originalbetrag und - falls vorhanden - Gebührenbetrag in dasselbe Feld einzustellen.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verwendete Finanzdatenformate	Stand: 02.02.1998	Seite: 139

Nr.	Name	Format 13	Länge	Status	Bemerkungen
	Subfeld 3: (Soll-Betrag)	9	..15	M	Betrag in Kontowährung mit Komma als Dezimalzeichen (gem. SWIFT-Konventionen)
:90C:	Anzahl und Summe der Habenbuchungen		..23	K	Bei DFÜ-Übertragung Pflichtfeld wegen Abstimmsummen
	Subfeld 1: (Anzahl Habenbuchungen)	9	..5	M	
	Subfeld 2: (Währung)	X	3	M	Währungsschlüssel gem. ISO 4217
	Subfeld 3: (Haben-Betrag)	9	..15	M	Betrag in Kontowährung mit Komma als Dezimalzeichen (gem. SWIFT-Konventionen)

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 140	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Berechnung der Prüfziffer für interne Zuordnungsdaten

VIII.10 Berechnung der Prüfziffer für interne Zuordnungsdaten (Kunden-Referenznummer)¹⁶

(nach DIN ISO 7064, MOD 11,10)

VIII.10.1 Rechengang

Die internen Zuordnungsdaten (Kunden-Referenznummer) bestehen aus 12 Ziffern und einer einstelligen Prüfziffer, bilden also eine 13stellige Zeichenkette. Diese Kette wird Zeichen für Zeichen von links nach rechts verarbeitet.

Mit dem Index $j = 1..n$ (wobei n die Anzahl der Zeichen in der Kette einschließlich Prüfziffer ist) und mit dem Anfangswert $P_1 = M$ für $j = 1$ berechnet man

$$S_j = P_j I_{(M+1)} + a_{(n-j+1)}$$

$$P_{(j+1)} = S_j I_M \times 2$$

Dabei ist

I_M der Rest nach Division durch M ; falls dieser gleich Null ist, ist statt dessen Wert M einzusetzen.

$I_{(M+1)}$ der Rest nach Division durch $(M+1)$; hier wird der Rest niemals gleich Null

$a_{(n-j+1)}$ der Zeichenwert

Bei der Prüfung gilt die Kette als richtig, wenn $S_n = 1 \pmod{M}$ ist.

Zur Berechnung des Prüfzeichens wird a_1 so gewählt, daß $P_n I_{(M+1)} + a_1 = 1 \pmod{M}$ ist. Mit dem für a_1 gefundenen Wert werden die internen Zuordnungsdaten (Kunden-Referenznummer) ergänzt.

¹⁶ Entnommen aus „Richtlinien für einheitliche Zahlungsverkehrsvordrucke und Merkblätter für neutrale Zahlungsverkehrsvordrucke“.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Berechnung der Prüfziffer für interne Zuordnungsdaten	Stand: 02.02.1998	Seite: 141

VIII.10.2 Beispiel

Die internen Zuordnungsdaten (Kunden-Referenznummer) lauten 100845456115. Sie sind am rechten Ende zu ergänzen durch die Prüfziffer nach DIN ISO 7064, MOD 11,10.

♦ Rechnung

Schritt	Übertragenes Produkt		nächster Zeichenwert	Zwischensumme	Zwischensumme (mod 10) x 2 = Produkt	Produkt (mod 11) Übertrag
j	$P_j \downarrow_{11}$	+	$a_{(n-j+1)}$	$= S_j$	$S_j \downarrow_{10} \times 2 = P_{(j+1)}$	$P_{(j+1)} \downarrow_{11}$
1			2		3	4
1	10	+	1	= 11	$1 \times 2 = 2$	2
2	2	+	0	= 2	$2 \times 2 = 4$	4
3	4	+	0	= 4	$4 \times 2 = 8$	8
4	8	+	8	= 16	$6 \times 2 = 12$	1
5	1	+	4	= 5	$5 \times 2 = 10$	10
6	10	+	5	= 15	$5 \times 2 = 10$	10
7	10	+	4	= 14	$4 \times 2 = 8$	8
8	8	+	5	= 13	$3 \times 2 = 6$	6
9	6	+	6	= 12	$2 \times 2 = 4$	4
10	4	+	1	= 5	$5 \times 2 = 10$	10
11	10	+	1	= 11	$1 \times 2 = 2$	2
12	2	+	5	= 7	$7 \times 2 = 14$	3
13	3	+	8	= 1		
				(mod 10)		

Die gesuchte Prüfziffer ist 8.

♦ Erläuterungen

Der Ausgangswert, auf den im 1. Schritt der 1. Zeichenwert addiert wird, ist immer 10.

Zwischensumme (mod 10): Das Ergebnis der Rechenoperation in Sp. 2 wird durch 10 dividiert; der Divisionsrest (Einerstelle des Ergebnisses) ergibt die Zwischensumme $S_j \downarrow_{10}$.

Ist dieser Wert = 0, ist statt dessen der Wert 10 zu setzen.

Produkt (mod 11): Das Produkt in Sp. 3 wird durch 11 dividiert; der Divisionsrest ergibt den nächsten Berechnungsschritt.

Prüfziffer: Im letzten Berechnungsschritt ist der Übertrag auf den Wert 11 (= 1 (mod 10)) zu ergänzen. Der gefundene Zeichenwert ist die Prüfziffer. Ist der Übertrag aus Schritt 12 jedoch = 1, so ist die Prüfziffer = 0.

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 142	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Länderkennzeichen und Währungscode

VIII.11 Länderkennzeichen und Währungscode

Nachfolgend sind für ausgewählte Länder jeweils der Ländercode laut ISO 3166-1 sowie der Währungscode und die Anzahl der Währungsnachkommastellen laut ISO 4217 aufgelistet:

Ländername	Ländercode (numerisch)	Ländercode (Alpha-2)	Währungs- code	Nachkomma- stellen
Belgien	056	BE	BEF	0
Bulgarien	100	BG	BGL	2
Dänemark	208	DK	DKK	2
Deutschland	280 ¹⁷	DE	DEM	2
Finnland	246	FI	FIM	2
Frankreich	250	FR	FRF	2
Griechenland	300	GR	GRD	0
Großbritannien	826	GB	GBP	2
Island	352	IS	ISK	2
Irland	372	IE	IEP	2
Italien	380	IT	ITL	0
Japan	392	JP	JPY	0
Kanada	124	CA	CAD	2
Kroatien	191	HR	HRK	2
Liechtenstein	438	LI	CHF	2
Luxemburg	442	LU	LUF	0
Niederlande	528	NL	NLG	2
Norwegen	578	NO	NOK	2
Österreich	040	AT	ATS	2
Polen	616	PL	PLN	2
Portugal	620	PT	PTE	0
Rumänien	642	RO	ROL	2
Russische Föderation	643	RU	RUR	2
Schweden	752	SE	SEK	2
Schweiz	756	CH	CHF	2
Slowakei	703	SK	SKK	2
Slowenien	705	SI	SIT	2
Spanien	724	ES	ESP	0
Tschechien	203	CZ	CZK	2
Türkei	792	TR	TRL	2
Ungarn	348	HU	HUF	2
USA	840	US	USD	2
Euro	978	EU	EUR	2

¹⁷ Der neue Code 276 wird derzeit noch nicht verwendet, da der Code 280 im Kreditgewerbe gebräuchlicher ist.

Homebanking-Computer-Interface (HBCI)	Version: 2.0.1	Kapitel: VIII
Kapitel: Anlagen Abschnitt: Verweise auf verwendete Dokumente	Stand: 02.02.1998	Seite: 143

VIII.12 Verweise auf verwendete Dokumente

Die Verweise und weiterführenden Literaturhinweise sind nachfolgend nach Themenbereichen geordnet:

VIII.12.1 Allgemeines

1. ISO 639:1988: Code for the representation of names of languages
2. ISO 3166-1:1996: Code for the representation of names of countries and their subdivisions - Part 1: Country code
3. ISO 4217:1995: Codes for the representation of currencies and funds
4. ISO 8859-1:1987: Information processing - 8 bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1

VIII.12.2 Sicherheit

1. Kryptographische Verfahren des deutschen Kreditgewerbes für die Elektronische Unterschrift und für die Verschlüsselung im Rahmen der Kunde-Bank-Kommunikation
in: ZKA-Abkommen über die Datenfernübertragung zwischen Kunden und Kreditinstituten (DFÜ-Abkommen) v. 15.03.1995, Anlage 2
2. Schnittstellenspezifikation für die ec-Karte mit Chip, Zentraler Kreditausschuß, Stand 27.10.1995
3. ISO CD 9735-5: Electronic data interchange for administration, commerce and transport - (EDIFACT) - Application level syntax rules; Part 5: Security rules for batch EDI (Authenticity; Integrity and Non-repudiation of origin), SJWG, Release 1 1995-12-14 (noch nicht veröffentlicht)
4. ISO WD 9735-7: Electronic data interchange for administration, commerce and transport - (EDIFACT) - Application level syntax rules; Part 7: Security rules for batch EDI (Confidentiality), SJWG, Release 1.1 1995-10-18 (noch nicht veröffentlicht)
5. ISO CD 9735-9: Electronic data interchange for administration, commerce and transport - (EDIFACT) - Application level syntax rules; Part 9: Security key and certificate management (Message type - KEYMAN), SJWG, Release 1 1996-01-12 (noch nicht veröffentlicht)
6. ISO 9796: Information technology - Security techniques - Digital signature scheme giving message recovery
7. ISO 10116: Information technology - Modes of operation for an n-bit block cipher algorithm
8. ISO 10118-2: Information technology - Security techniques - Hash functions Part 2: Hash functions using an n-bit block cipher algorithm
9. [ISO 10118-3: Information technology - Security techniques - Hash functions Part 3: Dedicated hash functions, Draft, 1997](#)
10. ISO 10126: Banking - Procedures for message encipherment (wholesale)
11. ANSI X3.92-1981 (R1987): Data Encryption Algorithm

Kapitel: VIII	Version: 2.0.1	Homebanking-Computer-Interface (HBCI)
Seite: 144	Stand: 02.02.1998	Kapitel: Anlagen Abschnitt: Verweise auf verwendete Dokumente

12. ANSI X3.106-1983 (R1996): Data Encryption Algorithm, Modes of operation for the
13. ANSI X9.19-1996: Financial Institution Retail Message Authentication
14. ANSI X9.23-1995 (R1995): Financial Institution Encryption of Wholesale Financial Messages
15. EDIFACT Message Implementation Guidelines: Ciphred Text Message. CIPHER, SJWG; Working Draft Version, Paris September 16th 1994
16. EDIFACT Security Implementation Guidelines, Trade/WP.4/R.1026/Add.2, 22 February
17. MIG Handbook UN/EDIFACT Message KEYMAN (proposed draft), June 30, 1995
18. [R. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, vol. 21 no. 2, 1978.](#)
19. H. Dobbertin, A. Bosselaers, B. Preneel: „RIPEMD-160, a strengthened version of RIPEMD“, Fast Software Encryption - Cambridge Workshop 1996, LNCS, Band 1039, D. Gollmann, Ed., Springer-Verlag, 1996, S. 71-82
(<ftp://ftp.esat.kuleuven.ac.be/pub/COSIC/bosselaer/ripemd/>)

VIII.12.3 Transportmedienspezifische Festlegungen

1. Datex-J Rechnerverbund - EHKP Protokollhandbuch, Version 4.3 vom 18.10.1995, Deutsche Telekom AG, Zentrum MIV Darmstadt
2. Datex-J - X.29 Protokollhandbuch, 3. Ausgabe vom September 1993, Deutsche Telekom AG, Zentrum MIV Darmstadt
3. Functional Specifications for Bildschirmtext Terminals, Deutsche Telekom AG, Zentrum MIV Darmstadt
4. Funktionserweiterungen im Datex-J-Dienst - Technische Beschreibung der Datex-J Release 4.2/4.3, Stand: 26.6.1995, Deutsche Telekom AG, FTZ Darmstadt, Referat T24
5. Btx File Interchange Format (BtxFIF) for Transparent Mode, Deutsche Telekom AG, FTZ Darmstadt, Referat T25, Version 1.1, August 1992
6. Request for Comment (RFC) 791: Internet Protocol (IP), September 1981
7. Request for Comment (RFC) 793: Transmission Control Protocol (TCP), September 1981
8. Request for Comment (RFC) 1700: Assigned Numbers, Oktober 1994

Bezugsquelle für RFC-Dokumente: z.B. <ftp://ftp.eunet.de/pub>

VIII.12.4 Geschäftsvorfälle

1. Richtlinien für einheitliche Zahlungsverkehrsvordrucke und Merkblätter für neutrale Zahlungsverkehrsvordrucke