

Z E N T R A L E R K R E D I T A U S S C H U S S

MITGLIEDER: BUNDESVERBAND DER DEUTSCHEN VOLKSBANKEN UND RAIFFEISENBANKEN E.V. BERLIN • BUNDESVERBAND DEUTSCHER BANKEN E. V. BERLIN • BUNDESVERBAND ÖFFENTLICHER BANKEN DEUTSCHLANDS E. V. BERLIN • DEUTSCHER SPARKASSEN- UND GIROVERBANDE E. V. BERLIN-BONN • VERBAND DEUTSCHER HYPOTHEKENBANKEN E. V. BERLIN

Schnittstellenspezifikation für die Datenfernübertragung zwischen Kunde und Kreditinstitut gemäß DFÜ-Abkommen

Stand:

**12. August 2003
(Version 1.0)**

Änderungsverfolgung

Laufende Nummer (CR-Nr.)	Kapitel	Beschluss-Datum	Art*	Beschreibung	Änderung gültig ab

* F = Fehler; Ä = Änderung; K = Klarstellung; E = Erweiterung; L = Löschung

Inhaltsverzeichnis

1 Anlage 1 (Standards für die Kommunikation)	1
1.1 Anwendungsprotokoll Kunden-/Bankrechner	1
1.1.1 Remote-User-ID	1
1.1.2 Remote-Password	1
1.1.3 Remote-Filename	1
1.2 FTAM-Verfahrensspezifikation	3
1.2.1 Virtual Filestore	4
1.2.2 FTAM Units	7
1.2.3 Anwendungsschicht ACSE	11
1.2.4 Presentation Layer	12
1.2.5 Session Layer	13
1.2.6 Transport Layer	14
1.2.7 Network Layer	14
1.2.8 Literaturverzeichnis	16
1.3 Die Adressierung bei der DFÜ mit Kunden	18
1.3.1 Adressierung X.25	18
1.3.2 Verwendung der X.25 Call User Data	18
1.3.3 Transport-Selektor	18
1.3.4 Session-Selektor	18
1.3.5 Presentation-Selektor	19
1.3.6 Adressierung der Anwendungsebene (Application Entity Title)	19
1.3.7 Initiator-ID und Passwort	19
1.4 Auftragsartenkennungen	20
1.4.1 Kategorie 1: Standardisierte Auftragsarten	20
1.4.2 Kategorie 2: Systembedingte Auftragsarten	22
1.4.3 Kategorie 3: Reservierte Auftragsarten für den zwischenbetrieblichen Zahlungsverkehr/Dateiaustausch	23
1.4.4 Kategorie 4: Sonstige reservierte Auftragsarten unter Verwendung nicht standardisierter Formate und Verfahren	23
1.5 Fehlermeldungen/Fehlercodes	25
1.6 Betrieb über asynchrone Verbindungen und PAD	25
1.6.1 Anforderungen an das Verfahren	26
1.6.2 Kurzbeschreibung der Lösung	26
1.6.3 Spezifikation	26

1.6.3.1 Kontroll- und Dateneinheiten	26
1.6.3.2 Protokollabläufe	27
1.6.3.3 Mögliche Abläufe beim Austausch von Dateneinheiten	27
1.6.3.4 Konfigurationsparameter	30
1.6.3.5 Datenformate der Kontroll- und Dateieinheiten	30
1.6.3.6 Berechnung der Checksumme und Codierung der NSDU im 7- oder 8-bit Modus	32
1.6.3.7 Decodierung und Prüfung der NSDU	34
1.6.4 Abkürzungsverzeichnis	37
1.7 Kundenprotokoll - inhaltliche und formale Festlegungen	38
1.7.1 Inhaltliche Festlegungen	38
1.7.2 Formale Festlegungen	39
1.7.2.1 Protokollierung der Aktionen auf der Bankseite	39
1.7.2.2 Protokollierung der Fehler bei Unterschriftsprüfung	41
1.7.2.3 Dateianzeige	42
1.7.2.4 Unterstützung fremdsprachiger Kundenprotokolle	42
1.7.3 Liste der möglichen Meldungen inklusive Textnummer	44
1.7.4 Dateianzeige auf Kunden- und Bankseite	47
2 Anlage 2 (Standards für die Sicherheit)	49
2.1 Festlegungen / Symmetrischer Algorithmus	49
2.2 Kryptographische Verfahren des deutschen Kreditgewerbes für die Elektronische Unterschrift im Rahmen der Kunde-Bank-Kommunikation	51
2.2.1 Allgemeine Anforderungen	51
2.2.2 Elektronische Unterschrift der Version A003	52
2.2.2.1 Festlegungen	52
2.2.2.2 Definitionen	54
2.2.2.3 Voraussetzungen	54
2.2.2.4 Sicherung der Nachrichten	54
2.2.2.5 Formate	56
2.2.2.6 Beschreibung der Abläufe	57
2.2.2.7 Testdaten Elektronische Unterschrift	63
2.2.3 Elektronische Unterschrift der Version A004	69
2.2.3.1 Einleitung	69
2.2.3.2 RSA-Schlüsselkomponenten	69
2.2.3.3 Signatur-Algorithmus	71
2.2.3.4 Signaturverfahren gemäß DIN-Spezifikation	72
2.2.3.5 Referenzen	76
2.2.3.6 Signaturformat der ZKA-Chipkarte bei DFÜ mit Kunden	77
2.2.3.7 Testdaten Elektronische Unterschrift	80
2.3 Verschlüsselung	81
2.3.1 Allgemeine Anforderungen	81
2.3.2 Schaffung der Voraussetzungen für die verschlüsselte Kommunikation	81
2.3.3 Vorbereitung der Verschlüsselung / Public-Key-Austausch	81

2.3.4 Ver- und Entschlüsselung	84
2.3.4.1 Vorgänge beim Sender	84
2.3.4.2 Vorgänge beim Empfänger	86
2.3.5 Beispielhafte Beschreibung der Abläufe	88
2.3.6 Interne Datenformate der Funktion „Verschlüsselung“	93
2.3.6.1 PDEK und DES-Schlüssel (DEK)	93
2.3.6.2 EDEK	94
2.3.6.3 Exponent	95
2.3.6.4 Modulo	96
2.3.6.5 Testdaten Verschlüsselung	97
2.3.7 Liste der reservierten Antwortcodes	98
2.3.8 Abkürzungsverzeichnis	99
3 Anlage 3 (Datenformate)	100
3.1 Inlandszahlungsverkehr	100
3.1.1 DTAUS0: Zahlungsverkehrssammelauftrag Diskettenformat	100
3.1.2 DTAUS: Zahlungsverkehrssammelauftrag Magnetbandformat	110
3.1.3 DTAUS: Lastschriftsammelauftrag electronic cash	118
3.1.4 DTAUS: Lastschriftsammelauftrag Maestro	128
3.1.5 DTAUS: Lastschriftsammelauftrag POZ	139
3.2 Auslandszahlungsverkehr	145
3.3 Wertpapiergeschäft	177
3.3.1 MT 513 Ausführungsanzeige	177
3.3.2 MT 515 Wertpapierabrechnung	195
3.3.3 MT 535 Depotaufstellung	215
3.3.4 MT 536 Depotumsatzinformation	231
3.4 Akkreditivgeschäft	244
3.4.1 DTAEA Export-Akkreditiv-Avisierung und –änderung (Bank an Kunde)	244
3.4.2 DTALC Import-Akkreditiveröffnungs- und Änderungsaufträge (Kunde an Bank)	252
3.4.3 DTALCR Ausführungsbestätigungen von Import-Akkreditiveröffnungen und –änderungen (Bank an Kunde)	265
3.5 Tageskontoauszugsinformationen	277
3.5.1 MT 940 Kontoauszugsdaten	278
3.5.2 MT 942 Kontoumsatzavis	290

Für alle SWIFT-Formate gilt -soweit nicht anders definiert- der SWIFT-Zeichensatz

1 Anlage 1 (Standards für die Kommunikation)

1.1 Anwendungsprotokoll Kunden-/Bankrechner

Das Protokoll beschreibt die Belegung der Request-Parameter Remote-User-ID, Password und Filename sowie der Anwendungsfehlermeldungen. Nicht genutzte Stellen dieser Felder werden mit Blanks aufgefüllt.

1.1.1 Remote-User-ID

Bankspezifische User-ID (8 Bytes alphanummerisch, beginnend mit einem Alphazeichen)

1.1.2 Remote-Password

Byte 1 – 8: Bankenspezifisches Password (8 Bytes alphanummerisch)

Byte 9 – 16: Bankenspezifisches neues Password (8 Bytes alphanummerisch); nur bei Auftragsarten INI und PWA

1.1.3 Remote-Filename

Das Feld enthält die inhaltliche Beschreibung des Transferauftrages und gegebenenfalls auftragsspezifische Daten. Nur Byte 1 bis 44 werden genutzt. Die einzelnen Parameter sind durch Punkte voneinander getrennt. Aus Kompatibilitätsgründen beim Empfänger-Betriebssystem ist das erste Byte eines Qualifiers immer ein Alphazeichen. Die Grundstellung für nicht belegte Stellen ist 'N'. Der Aufbau ist:

PV.Kunden-ID.Auftragsart.Auftragsattribut[.Auftragsnummer] [.Auftragsparameter]

Erläuterung:

- PV (2 Bytes alphanummerisch):
Versionsnummer des Anwendungsprotokolls; zur Zeit konstant 'A3'
- Kunden-ID (8 Bytes alphanummerisch):
Bankspezifische Kunden-ID
- Auftragsart-Kennung (3 Bytes alphanummerisch, siehe 1.4 Auftragsartenkennungen)
- Auftragsattribut (5 Bytes alphanummerisch):

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Byte	Inhalt	Auswahlmöglichkeiten
1	Dateiart	O = Originaldatei mit zugehöriger Unterschriftsdatei U = Unterschriftsdatei D = Originaldatei ohne zugehöriger Unterschriftsdatei B = Originaldatei und EU-Datei in einer physikalischen Datei P = Protokolldatei Y = Dummy-Datei
2	Komprimierungsart ¹	N = Keine Komprimierung F = FLAM-Komprimierung Z = PKZIP-Komprimierung X = x-Press-Komprimierung ... Die zum Einsatz kommenden Komprimierungsprodukte werden durch die ZKA-Buchstabenkennungen festgelegt.
3	Verschlüsselungsart	N = Keine Verschlüsselung H = Hybrid-Verfahren DES/RSA R = RSA
4	Reserve	
5	Reserve	

- **Auftragsnummer (4 Bytes alphanummerisch):**
Je Kunde eindeutige Auftragsnummer für die Übertragungsrichtung Kunde/Bank. Dient als Ordnungsbegriff bei der PC-Host-Kommunikation, insbesondere beim Protokollabruf und bei der Synchronisation von Original- und Unterschriftsdatei.

Byte	Inhalt
1	A
2	laufende Nummer des Kunden-DFÜ-PCs
3-4	2 Stellen alphanummerisch (werden aufsteigend vergeben)

- **Auftragsparameter:**
Auftragsspezifische weitere Parameter, falls für die Auftragsart erforderlich bzw. zugelassen. Zur Zeit:

Auftragsart	Auftragsparameter
-------------	-------------------

¹ Sofern nichts anderes vereinbart, ist das FLAM-Verfahren das Standard-Komprimierungsverfahren.

Auftragsart	Auftragsparameter
STA	optional Datum-von Datum-bis (VJJMMTT.BJJMMTT)
VPK	Kennung für User-ID des Kunden, der VPK-Auftrag unterschrieben hat Byte 1: U (Kennung für User-ID) Byte 2 – 9: User-ID
alle verschlüsselt zu übertragenden Dateien	Verschlüsselungs-Public-Key-Hashwert (33 Bytes alphanummerisch): Byte 1: H (Kennung für Hashwert) Byte 2-33: Verschlüsselungs-Public-Key in Hex-Darstellung

1.2 FTAM-Verfahrensspezifikation

Als Grundlage für die DFÜ-Kommunikation mit Kunden dienen folgende nationale und internationale Standards:

- Profile A/111 [38]
- FTAM [18]
- ASN.1 [14], [15]
- ACSE [16], [17]
- Presentation Service [12] und Protocol [13]
- Session Service [10] und Protocol [11]
- Profile T/331 [37]
- Transport Service [8] und Protocol [9]
- Datex-P [2]
- OSI-Adressierung [4]

Die internationalen Standards der ISO sind in vielen Teilen bewußt allgemein gehalten, um möglichst viele verschiedene Anwendungsszenarien abzudecken und um zukünftige Weiterentwicklungen nicht zu behindern.

Daher werden zusätzlich bestimmte Richtlinien zur Benutzung dieser Standards für bestimmte Anwendergruppen definiert. Diese Richtlinien, Functional Standards oder Profile genannt, werden von verschiedenen Normungsgremien erarbeitet (z. B. SPAG, CEN/CENELEC, ISO).

Das Profile A/111 des Guide to Use of Standards (GUS Rev. 3.1), herausgegeben von der Standards Promotion and Applications Group (SPAG), definiert einen Subset der Funktionen in den Ebenen 5 bis 7 einer FTAM-Anwendung. Dieses Profil wurde von der europäischen Normungsorganisation CEN/CENELEC in Abstimmung mit CEPT als europäische Vornorm

ENV 41 204 [38] verabschiedet. Dieser Subset von OSI-Session, OSI-Presentation, OSI-ACSE und FTAM ist die Grundlage für den Filetransfer bei der DFÜ-Kommunikation mit Kunden.

Das ebenfalls von SPAG herausgegebene Profil T/31 X befaßt sich mit der Netzwerkverbindung und dem darauf aufsetzenden Transportprotokoll. Dieses Profil wurde ebenfalls als Vornorm ENV 41 104 [37] von CEN/CENELEC in Abstimmung mit CEPT übernommen und dient als weitere Grundlage für die DFÜ-Kommunikation mit Kunden.

Abbildung 1.1 zeigt den Zusammenhang der verschiedenen Protokollschichten in einer Übersicht.

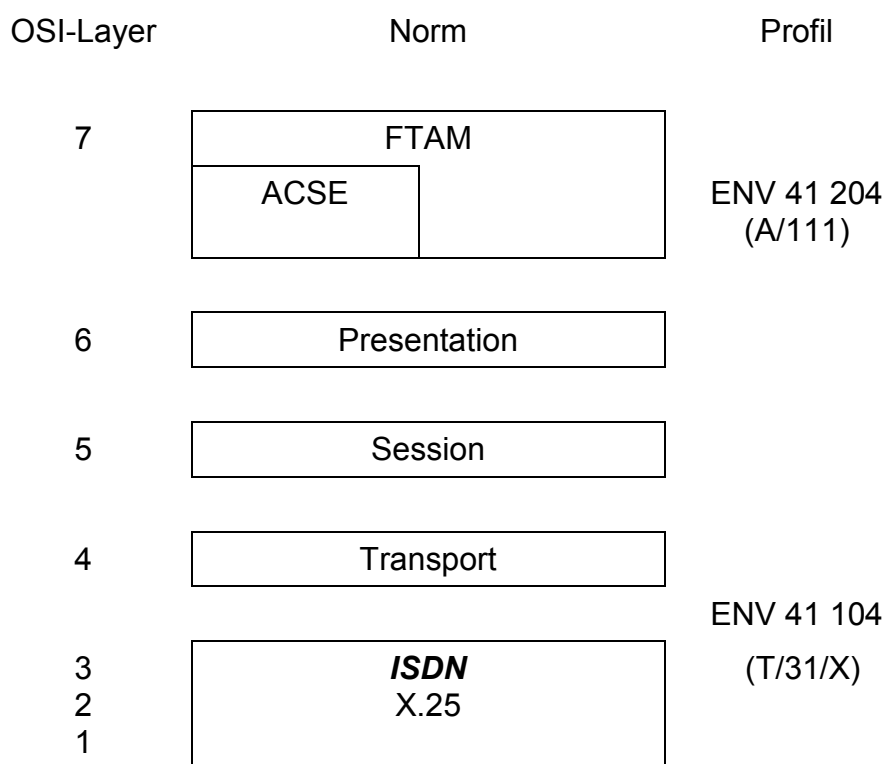


Abbildung 1.1 ISO OSI Schichtmodell

1.2.1 Virtual Filestore

Die Art der Dateihaltung und der Zugriff auf die Dateien ist bei den verschiedenen realen DV-Systemen sehr unterschiedlich. Um unterschiedliche reale Systeme miteinander zu verbinden, wird daher ein gemeinsames Modell zur Beschreibung von Dateien und ihrer Attribute benötigt. Dieses Modell wird Virtual Filestore genannt.

Rollenverteilung: Eine FTAM-Verbindung wird immer von einem FTAM-Initiator initiiert. Im Rahmen der DFÜ mit Kunden ist dies immer der Kunde. Der dazugehörige Partner im Remote-System ist ein FTAM-Responder. Der FTAM-Initiator kann sowohl Sender von Daten wie auch Empfänger sein. Gleiches gilt für den FTAM-Responder. Der FTAM-Initiator kann durch die Dienstleistung des FTAM-Responders auf den Virtual Filestore des Partnersystems zugreifen (siehe Abbildung 1.2).

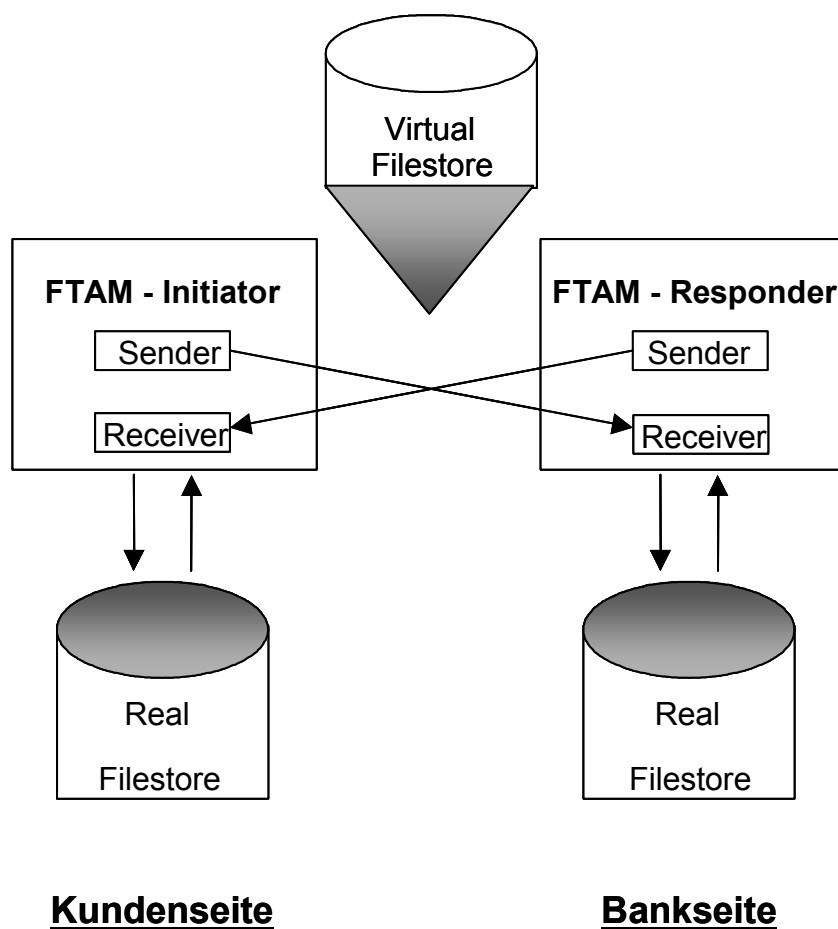


Abbildung 1.2 FTAM-Initiator/Responder

Jeder Partner in einem FTAM-Verbund bildet seine remote zugänglichen Daten bzw. Datenbereiche auf einem Virtual Filestore ab. Ein Virtual Filestore kann eine oder mehrere Dateien, ganze Directories (auch hierarchisch) oder sogar die gesamten Dateien auf dem Peripheriespeicher eines Systems beinhalten.

Dateistruktur:

Bei FTAM wird zur Zeit nur das File-Model hierarchical² verwendet. Bei diesem Modell besteht ein File aus verschiedenen Zugriffseinheiten, die File Access Data Units (FADU) genannt werden. Bei der DFÜ mit Kunden besteht eine Datei nur aus einer FADU, die nur die

² Object Identifier: {iso standard 8571 file-model (3) hierarchical (1)}.

Data Unit (DU) des Root-Knotens beinhaltet. Diese Data Unit wird in einzelnen Data Elements (DEs), stellenweise auch Strings genannt, übertragen.

Filenamen:

Nach ISO 8571 [20] besteht der Filename aus einem Vektor von GraphicStrings. Es werden Filenamen bis zu einer maximalen Länge von 44 Charakteren verwendet.

Der Filename muss nach ISO codiert [28] sein; EBCDI-Code ist nicht erlaubt.

FTAM Dateistruktur (Constraint Set):

Das Profile A/111 [38] unterstützt nur die Struktur unstructured³. Das bedeutet, dass nur auf die Datei als Ganzes zugegriffen werden kann und nicht auf Teile der Datei. Diese Zugriffsart entspricht der Anwendung bei der DFÜ mit Kunden.

Dateiinhalt (FTAM Document Type):

Das Profile A/111 [38] erlaubt nur die Document Types ISO FTAM unstructured text (FTAM-1) und ISO FTAM unstructured binary (FTAM-3).

FTAM-1 läßt die Übertragung beliebiger Textdateien zu. Für die Übertragung von Textdateien mit fester Satzlänge wird die Satzlänge der jeweiligen Datei an der Aufrufchnittstelle als Parameter übergeben.

FTAM-3 läßt die Übertragung von beliebigen Binärdateien zu. Diese können bei der DFÜ mit Kunden dann auch komprimiert (Komprimierung in der Anwendung, nicht in FTAM) sein.

Nach dem Profile A/111 ist für FTAM-3 die *string significance* nur mit dem Wert not significant zugelassen, wodurch keine Abbildung der Data Elements auf Sätze mehr möglich ist.

Die Satzstruktur wird daher aus den mitübertragenen Satzlängefeldern vor jedem Datensatz grundsätzlich nicht in FTAM rekonstruiert.

Die Rekonstruktion erfolgt vielmehr empfängersystemspezifisch auf Basis der Auftragsarten-Kennung des Kunden-/Bankrechner-Protokolls (siehe Kapitel Kontroll- und Dateneinheit). Dabei sind bei Binärdateien variabler Satzlänge folgende Alternativen möglich:

Alternative 1 (Userexits): Unmittelbar nach dem Empfang der Datei, noch während der FTAM-Verbindung, am Ende des FTAM-Select-Regimes, wird die Nachbehandlung (Rekonstruktion) der Dateien unter Nutzung eines entsprechenden Userexits durchgeführt. Voraussetzung ist hierfür, dass das jeweilig eingesetzte FTAM-Produkt die gewünschten Userexits anbietet.

Alternative 2 (Anwendung): Die Nachbehandlung (Rekonstruktion) erfolgt erst nach Beendigung der FTAM-Verbindung am Ende des FTAM-Regimes durch empfängersystemspezifische Anwendungen.

FTAM Zugriffsumgebung (Access Context):

Durch das Profile A/111 wird nur UA - Unstructured All Data Units Access Context - unterstützt. Das bedeutet, dass nur der Inhalt der Datei (keine Strukturinformation) - und dieser nur im ganzen (nicht in Teilen) - zugreifbar ist. Dieser Access Context korrespondiert mit der FTAM Dateistruktur (Constraint Sets) und ist für die Anwendungen bei der DFÜ mit Kunden ausreichend.

³ Object Identifier: {iso standard 8571 constraint-set (4) unstructured (1)}.

FTAM Dateiattribute (File Attributes):

Von der Kernel Group werden folgende Attribute benötigt:

- filename (siehe "Filename" in Kapitel 1.2.1 Virtual Filestore)
- permitted actions: replace, extended, read
- contents type (beschränkt auf Document Type Format)

Von der Storage Group, der Security Group und der Private Group werden keine Attribute benötigt.

1.2.2 FTAM Units

FTAM File Service:

Der External File Service ist in die Functional Units U1 bis U8 unterteilt, welche wiederum den fünf Dienstklassen (T, A, M, TM, U) zugeordnet sind. Der Internal File Service ist in die Functional Units U9 und U10 unterteilt.

Bei der DFÜ mit Kunden wird die Dienstklasse (Service Class) File Transfer Class (T) mit folgenden Functional Units benötigt:

Functional Unit	
U1	Kernel
U2	Read
U3	Write (nur write replace genügt)
U5	Limited File Management (optional in A/111)
U7	Grouping
U9	Recovery (Class 3) (optional in A/111)

Für die DFÜ mit Kunden wird U5 benötigt, da Files remote vom Sender angelegt werden. U9 wird im Zusammenhang mit PAD-Verbindungen benötigt.

Folgende dateibezogene Aktionen werden bei DFÜ mit Kunden verwendet:

- Select File
- Create File (in A/111 nur optional)
- Open File
- Close File
- Deselect File

Von den unterschiedlichen Zugriffsarten werden folgende benötigt:

- Read

- Extend
- Write replace

FTAM Benutzung:

Mit dem ordnungsgemäßen Verbindungsabbau der FTAM-Verbindung (F-TERMINATE positiv quittiert) geht die Verantwortung auf den Empfänger der Datei über.

FTAM Protocol:

Folgende FTAM Protocol Data Units werden beim Kunden verwendet:

- F-Initialize FPDU
- F-Terminate FPDU
- F-U-Abort FPDU
- F-Select FPDU
- F-P-Abort FPDU
- F-Create FPDU
- F-Deselect FPDU
- F-Open FPDU
- F-Close FPDU
- F-Begin-Group FPDU
- F-End-Group FPDU
- F-Read FPDU
- F-Write FPDU
- F-Data-End FPDU
- F-Transfer-End FPDU
- F-Recover FPDU
- F-Cancel FPDU

Im Folgenden werden sie mit den verwendeten Parametern aufgelistet, wobei das Feld Status folgende Bedeutung hat:

Status	Bedeutung
m1	Pflicht (mandatory) im Standard (FTAM, ACSE, Presentation, Session)
m2	Pflicht im Profile A/111 (ENV 41 204) [38]
m3	Pflicht bei der DFÜ mit Kunden
d	Für dieses Feld ist ein Defaultwert definiert. Falls bei Wert keine Einschränkung ge-

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Status	Bedeutung
	nannt ist, muss dieses Feld voll unterstützt werden.
s	Unterstützt (supported)
°	Optional (optional). Die Syntax muss unterstützt werden, die Semantik ist optional.
–	Nicht verwendet
x/y	x = Status für Initiator, y = Status für Responder

Protocol Data Unit	Status	Wert
Parameter		
F-Initialize	m1	
protocol-Version	d	version-1
presentation-context-management	d	false
service-class	d	transfer-class
functional-units	m1	
attribute-groups	d	
ftam-quality-of-service	m1	
contents-type-list	m2	
initiator-Identity	m2	GraphicString (maximal 8 Zeichen)
account	°	
filestore-password	m2/°	GraphicString (maximal 8 Zeichen)
checkpoint-window	d	bei Passwortänderung 9 bis 16 Zeichen
action-result	d	
diagnostic	m2	
diagnostic-type	m1	
error-identifier	m1	
error-observer	m1	
error-source	m1	
further-details	m2	
F-Begin-Group	m1	
Threshold	m1	
F-End-Group	m1	
(no parameters)		
F-Create	m3	
override	d	
initial-attributes	m1	filename only
create-password	m2/°	
request-access	m1	
access-passwords	m2/°	
concurrency-control	°	
account	°	
state-result	d	

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Protocol Data Unit	Status	Wert
Parameter		
action-result	d	
Diagnostic	m2	
F-Open	m1	
processing-mode	d	replace
contents-type	m1	FTAM-1 und FTAM-3
concurrency-control	°	
enable-fadu-locking	d	false
activity-identifier	°	
recovery-mode	d	
state-result	d	
action-result	d	
diagnostic	m2	
state	°	
F-Write	m2	
file-access-data-unit-operation	m1	replace
file-access-data-unit-identity	m1	first
F-Data-End	m1	
action-result	d	
diagnostic	m1	
F-Transfer-End	m1	
action-result	m1	
diagnostic	m2	
F-Cancel	m1	
action-result	d	
diagnostic	m2	
F-Close	m1	
action-result	d	
diagnostic	m2	
F-Deselect	m1	
action-result	d	
charging	°	
diagnostic	m2	
F-Terminate	m1	
charging	°	
F-U-Abort	m1	
action-result	d	
diagnostic	m2	
F-P-Abort	m1	
action-result	d	
diagnostic	m2	

Zusätzlich

Protocol Data Units	Status	Wert
Parameter		
F-Select	m1	
attributes	m1	
requested-access	m1	
access-passwords	◦	
concurrency-control	◦	
account	◦	
state-result	d	
action-result	d	
diagnostic	m2	
F-Recover	m3	bei PAD-Verbindungen
activity-identifier	m1	
bulk-transfer-numer	m1	
requested-access	m1	
access-passwords	◦	
recovery-point	d	
contents-type	m1	
state-result	d	
action-result	d	
dagnostic	s	
presentation-action	d	
F-Read		
file-access-data-unit-identify	m1	
access-context	m1	

1.2.3 Anwendungsschicht ACSE

Folgende Association Control Service Elements werden verwendet:

- A-Associate-Request (AARQ) APDU⁴
- A-Associate-Response (AARE) APDU
- A-Associate-Release-Request (RLRQ) APDU
- A-Associate-Release-Response (RLRE) APDU
- A-Abort (ABRT) APDU

⁴ APDU = Application Package Data Unit

Im folgenden werden sie mit den verwendeten Parametern aufgelistet.

Protocol Data Units		Status	Wert
Parameter			
A-Associate-Request	m		
protocol-Version	d		version-1 (0)
application context name	m1		iso standard 8571 application context (1) iso-ftam (1)
calling AP title	m2		1 3 9999 1 ftam-nil-ap-title (7)
calling AE Qualifier	m2		Integer
called AP title	m2		1 3 9999 1 ftam-nil-ap-title (7)
user information	m2		F-Initialize-Request FPDU
A-Associate-Response	m		
protocol version	d		version-1 (0)
result	m2		
responding AP title	m2		1 3 9999 1 ftam-nil-ap-title (7)
responding AE Qualifier	m2		Integer
application context name	m1		iso standard 8571 application context (1) iso-ftam (1)
user information	m2		F-Initialize-Response FPDU
A-Associate-Release Request	m		
user information	m2		F-Terminate-Request FPDU
A-Associate-Release- Response	m		
user information	m2		F-Terminate-Response FPDU
A-Abort	m		
abort source	m1		
user information	m2		F-P-Abort

1.2.4 Presentation Layer

Es kommt ein Presentation Layer nach dem in ISO 8822 [12] definierten Service und gemäß dem in ISO 8823 [13] definierten Protokoll zum Einsatz.

- Funktionsumfang:
Es werden nur die Kernel-Funktionen benötigt.
- Kontexte:
Es werden folgende, in Abstract Syntax Notation 1 (ASN.1) [14] definierte Datenstruktu-

ren bearbeitet: ISO 8650-ACSE⁵, ISO 8571-FTAM PCI⁶, FTAM unstructured binary abstract syntax⁷

- Kodierungsregeln:
Die Datenstrukturen werden nach den Basic Encoding Rules for ASN.1 [15] codiert⁸.
- Wertebereiche:
Für das Encoding gelten folgende Einschränkungen:

Taglänge:	maximal 2 Oktetts
Längenfeld:	maximal 5 Oktetts
Inhalt:	maximal 8k Oktetts

1.2.5 Session Layer

- Namenskonventionen des Session-Selektors:
Der Session-Selektor kann maximal aus 16 Oktetts bestehen. Sein Wert ist im Kapitel 1.3: „Die Adressierung bei der DFÜ mit Kunden“ festgelegt.
- Genutzter Funktionsumfang:

Functional Unit	Support Level	Bemerkung
kernel	m1	
half-duplex	–	
duplex	m2	wird verwendet
negotiated release	–	
typed data	–	
capability data exchange	–	
minor synchronize	m3	bei FTAM Recovery (PAD)
major synchronize	–	
resynchronize	◦	bei Restart
exceptions	–	
activity management	–	

- Verwendete Tokens

⁵ Object Identifier: {joint-iso-ccitt association-control (2) abstract-syntax (1) apdus (0) version 1 (1)}.

⁶ Object Identifier: {iso standard 8571 abstract-syntax (2) ftam-pci (1)}.

⁷ Object Identifier: {iso standard abstract-syntax (2) unstructured-binary (4)}.

⁸ Object Identifier: {joint-iso-ccitt (2) asnl (1) basic-encoding (1)}.

Token	Support Level	Bemerkung
synchronize minor	◦	bei FTAM Recovery oder Restart

- Protokoll Optionen

Protocol Options	Support Level	Bemerkung
basic concatenation	m1	
segmenting	◦	

- Wertebereiche:
Die maximale Länge der SPDUs ist entsprechend 8 k Oktetts der TSDU definiert.
- User Data:
Die User Data enthalten die Connect-Request-PPDU der Presentation Layer.

1.2.6 Transport Layer

- Namenskonvention des Transport-Selektors:
Der Transport-Selektor darf maximal 32 Oktetts lang sein. Sein Wert ist im Kapitel 1.3: „Die Adressierung bei der DFÜ mit Kunden“ festgelegt.
- Verwendete Protokollklasse(n):
Auf den beteiligten Systemen muss das Transportprotokoll Class 0 oder die beiden Klassen Class 0 und Class 2 implementiert sein.
- Verwendung der User Data:
User Data werden nicht verwendet.
- Recordlänge und Nachrichtenlänge:
Als Recordlängen sind 128, 256, 512, 1024, 2048, 4096 und 8192 Oktetts zugelassen.
Die maximale Nachrichtenlänge muss mindestens 8 k Oktetts betragen.

1.2.7 Network Layer

An der Kommunikationsstelle des Kunden ist ein Datex-P10-Hauptanschluss, alternativ ein PAD-Anschluss erforderlich.

- Datex-P10-Hauptanschluss:
Zwischen der Kommunikationsstelle der Kunden und der Bank werden gewählte virtuelle Verbindungen (SVC) aufgebaut. Die verfügbare Datenrate und die Anzahl der möglichen Verbindungen sind so auszulegen, dass einem Verbindungsaufbauwunsch der Bank in der Regel entsprochen wird.
Bei Verbindungsaufbau auszuhandelnde Leistungsmerkmale
Anrufe der Kunden an die Bank werden ohne das Dienstmerkmal „Gebührenübernahme“ durchgeführt.
Eine Teilnehmerbetriebsklasse (Closed User Group) wird zur Zeit nicht vorgesehen.

Verwendung der Call User Data (CUD)

Das X.25-Feld für CUD wird einheitlich mit 01 00 00 00 besetzt.

- PAD-Anschluss:
Für die Kommunikation über PAD-Anschluss wird ein gesondertes Sicherungsprotokoll verwendet. Diese Spezifikation ist den Standards für die Kommunikation (Kapitel 1.6 „Betrieb über asynchrone Verbindungen und PAD“) beigefügt. Das Verfahren ist als Teil der Schicht 3 oberhalb der X.25-Schnittstelle angesiedelt.

1.2.8 Literaturverzeichnis

- [1] DATEL-Handbuch, 2. Auflage April 1985. Herausgegeben vom Fernmeldetechnischen Zentralamt 6100 Darmstadt.
- [2] DATEX-Handbuch, 2. Auflage August 1988. Herausgegeben vom Fernmeldetechnischen Zentralamt 6100 Darmstadt.
- [3] ISO 7498, Information processing systems – Open Systems Interconnection – Basic reference model.
- [4] ISO/DIS 7498-3, Information processing systems – Open Systems Interconnection – Part 3: Naming and addressing.
- [5] ISO 8509, Information processing systems – Open Systems Interconnection – Service conventions.
- [6] ISO 8208, Information processing systems – Data Communications – X.25 packet level protocol for DTE. Version 1985_03_27.
- [7] ISO 8348, Information processing systems – Data Communications – Network Service definition. Version 1985_03_27.
- [8] ISO 8072, Information processing systems – Open Systems Interconnection – Transport Service Specification. Version 1986.
- [9] ISO 8073, Information processing systems – Open Systems Interconnection – Transport Protocol Specification. Version 1986.
- [10] ISO 8326, Information processing systems – Open Systems Interconnection – Basic connection session service definition.
- [11] ISO 8327, Information processing system – Open Systems Interconnection – Basic connection oriented session protocol specification.
- [12] ISO 8822, Information processing system – Open Systems Interconnection – Connection oriented presentation service definition.
- [13] ISO 8823, Information processing systems – Open Systems Interconnection – Connection oriented presentation protocol specification.
- [14] ISO 8824, Information processing systems – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1).
- [15] ISO 8825, Information processing systems – Open Systems Interconnection – Basic encoding rules for Abstract Syntax Notation One (ASN.1).
- [16] ISO 8649, Information processing systems – Open Systems Interconnection – Service definition for the Association Control Service Element.
- [17] ISO 8650, Information processing systems – Open Systems Interconnection – Protocol specification for the Association Control Service Element.
- [18] ISO 8571, Information processing systems, Open Systems Interconnection – File Transfer, Access and Management –.
- [19] ISO 8571 Part 1, Information processing systems, Open Systems Interconnection – File Transfer, Access and Management – Part 1: General introduction.
- [20] ISO 8571 Part 2, Information processing systems, Open Systems Interconnection – File Transfer, Access and Management – Part 2: Virtual filestore definition.
- [21] ISO 8571 Part 3, Information processing systems, Open Systems Interconnection – File Transfer, Access and Management – Part 3: File service definition.
- [22] ISO 8571 Part 4, Information processing systems, Open Systems Interconnection – File Transfer, Access and Management – Part 4: File protocol specification.
- [23] ISO 646, Information processing – ISO 7_bit coded character set for information interchange
- [24] ISO 2022, Information processing – ISO 7_bit and 8_bit coded character sets – Code extension techniques.

- [25] ISO 4873, Information processing – ISO 8_bit code for information interchange – Structure and rules for implementation.
- [26] ISO 6429, Information processing – ISO 7_bit and 8_bit coded character sets – Additional control functions for character-imaging devices.
- [27] ISO 6937 Part 2, Information processing – Coded character sets for text communication – Part 2: Latin alphabetic and nonalphabetic graphic characters.
- [28] ISO 8859_1, Information processing – 8_bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1.
- [29] ISO 2375, Data processing – Procedure for registration of escape sequences.
- [30] ISO DIS 8227 edition 1985, Information processing – Data encipherment – Specification of algorithm DEA 1.
- [31] ISO 8372, Information processing – Modes of operation for a 64_bit block cipher algorithm.
- [32] ISO 8730, Banking – Requirements for message authentication (wholesale).
- [33] ISO 8732, Banking – Key management (wholesale).
- [34] CCITT Recommendation X.224 –.
- [35] CCITT Recommendation X.410 – Message Handling Systems – Remote Operations and Reliable Transfer Server (1984).
- [36] CEN/CENELEC/CEPT, M_IT_02 – Directory of functional standards – (For interworking in an OSI Environment).
- [37] CEN/CENELEC/CEPT, ENV 41 104 – Information Systems Interconnection – Packet Switched Data Networks – Permanent access (T/331).
- [38] CEN/CENELEC/CEPT, ENV 41 204 – Simple file transfer (A/111), 23.02.88.
- [39] National Bureau of Standards (NBS) - Implementors Agreements – Draft Stable Document, Vers Okt. 87.
- [40] Standard Promotion and Application Group (S.P.A.G.) – Guide to the Use of Standards.
- [41] UK Government OSI Profile V3.0.
- [42] S.W.I.F.T Benutzerhandbuch
- [43] Ergebnisniederschrift der Sitzung des ZKA-Arbeitskreises „Belegloser Auslandszahlungsverkehr“ vom 20.10.1988.
- [44] Datenverschlüsselung – Festlegung des Algorithmus DEA 1 – ISO/DIS 8227 Ausgabe 1985.

1.3 Die Adressierung bei der DFÜ mit Kunden

Die Adressierung der Protokoll-Instanzen erfolgt nach den Prinzipien des Referenz-Modells, d. h. eine Instanz der Schicht (N) wird über die Adresse des service access point (SAP) der Schicht (N - 1) erreicht. Für die Anwendungen der DFÜ-Kommunikation mit Kunden wird eine feste Adressen-Struktur verwendet.

Ein Virtual Filestore wird über die Adresse des Presentation-Service-Access-Point (PSAP) gegebenenfalls in Verbindung mit der Initiator-ID selektiert.

Die PSAP-Adresse besteht aus der NSAP-Adresse, den Werten des T-Selektors, des S-Selektors und des P-Selektors. Die NSAP-Adresse wird hier durch die Datex-P-Rufnummer repräsentiert.

Im Rahmen der DFÜ mit Kunden sind die NSAP-Adresse (Datex-P-Rufnummer), der T-, S- und P-Selektor sowie auch der Application Entity Title von der Bank fest anzulegen. Die Auswahl eines kundenspezifischen Virtual Filestore geschieht hierbei über die Initiator-ID, die durch die Bank je Kommunikationstelle eindeutig vorgegeben wird.

Die folgenden Detailfestlegungen sind als Empfehlung zu verstehen. Jede Bank kann nach eigenen Kriterien die eigene Adresse und die Adressen der Kunden neu definieren. Es ist ratsam, die Selektoren der Schichten mit unterschiedlichen Namen zu belegen.

1.3.1 Adressierung X.25

Da die volle OSI-Adressierung erst mit der X.25-Version von 1984 eine weite Verbreitung gefunden hat, ist die NSAP-Adresse vorerst nur durch die X.25 Adresse (DTE-Nummer) zu bilden.

1.3.2 Verwendung der X.25 Call User Data

Zur Adressierung des OSI-Transportprotokolls ist der hexadezimale Wert 01 00 00 00 mit der Satzlänge 0 vorgesehen.

1.3.3 Transport-Selektor

Der Transport-Selektor besteht aus bis zu 32 Oktetts.

- Wert des T-Selectors der Bank: EB-TSAP
(X'45 42 2D 54 53 41 50')
- Wert des T-Selectors des Kunden: EB-CLIENT
(X'45 42 43 4C 49 45 4E 54')

1.3.4 Session-Selektor

Der Session-Selektor besteht aus bis zu 6 Oktetts.

- Wert des S-Selectors der Bank: *darf nicht belegt werden*
- Wert des S-Selectors des Kunden: *darf nicht belegt werden*

1.3.5 Presentation-Selektor

Der Presentation-Selektor besteht aus maximal 4 Oktetts (39).

- Wert des P-Selectors der Bank: *darf nicht belegt werden*
- Wert des P-Selectors des Kunden: *darf nicht belegt werden*

1.3.6 Adressierung der Anwendungsebene (Application Entity Title)

Der Application Entity Title (AET) wird zur Selektion eines Virtual Filestore verwendet. Der AET besteht aus dem Application Process Title mit dem konstanten Wert „Iso (1) Identified-organisation (3) 9999 1 ftam-nil-ap-title (7)“ und einem Application Entity Qualifier (AEQ), der als Integer definiert ist. Damit ergibt sich konkret folgende Adressierung:

- AET: 1 3 9999 1 7
- AEQ zur Adressierung der Bank: Integerwert '0'
- AEQ zur Adressierung des Kunden: Integerwert wahlfrei zwischen -2^{31} und $2^{31}-1$

1.3.7 Initiator-ID und Passwort

Jeder Kommunikationsstelle wird eine Initiator-ID zugeordnet, die aus einer eindeutigen achtstelligen Kenn-Nummer der Kommunikationsstelle gebildet wird und der Kunden-ID aus der Bankparameterdatei entspricht.

Das Passwort wird in der verhashten Form verwendet.

Die Initiator-ID und das Passwort werden bei jedem Remote-Filezugriff angegeben. Sie dienen dem Remote-System zur Identifikation des Anrufers.

1.4 Auftragsartenkennungen

1.4.1 Kategorie 1: Standardisierte Auftragsarten

Kennung	Text	Satzlänge ⁹	Bits	Format
AAE	Senden Importakkreditiv Änderung	-1	7	DTALC / Änderung
AEA	Senden Exportakkreditive	-1	7	MT700, MT707, MT710 MT720, MT799
AIA	Senden Importakkreditive Avisierung	-1	7	DTALC / Avisierung
AKA	Abholen Importakkreditive	-1	7	DTALCR
AWV	AWV-Meldung senden	-1	7	EDIFACT
AZM	AZV im Magnetbandformat senden (Satzlänge variabel)	-1	8	DTAZV-Magnetband
AZV	AZV im Diskettenformat senden	256	7	DTAZV-Diskettenformat
AZ2	AZV im Magnetbandformat senden (Satzlängenfeld 2 Bytes)	64	8	DTAZV-Magnetband
AZ4	AZV im Magnetbandformat senden (Satzlängenfeld 4 Bytes)	64	8	DTAZV-Magnetband
DDG	Abholen Devisenhandelsbestätigung	-1	7	MT300
DHB	Senden Devisenhandelsbestätigung	-1	7	MT300
DTE	Eilauftrag (IZV im DTAUS0-Format) senden	128	7	DTAUS0
DTI	IZV-Datei abholen	128	7	DTAUS0
DTM	MCV-Datei abholen (Format analog MCV)	64	8	DTAUS-Magnetband
DTT ¹⁰	Telegrafische Zahlungen senden	128	7	DTAUS0
DTV	Zahlungsverkehrsdateien von Service- Rechenzentren senden	128	7	DTAUS0
DT2	MC2-Datei abholen (Format analog MC2)	64	8	DTAUS-Magnetband
DT4	MC4-Datei abholen (Format analog MC4)	-1	8	DTAUS-Magnetband
EAB	Exportakkreditive abholen	-1	7	DTAEA MT700, MT707, MT710 MT720, MT799
ECS	Senden electronic-cash Lastschriftdatei	128	7	DTAUS0
EDC	Senden Maestro-Lastschriftdatei	128	7	DTAUS0
EEA	EDIFACT abholen ASCII	-1	7	EDIFACT
EEZ	EDIFACT abholen EBCDIC	-1	8	EDIFACT

⁹ Die Satzlänge „-1“ bedeutet „variable Satzlänge“.

¹⁰ Diese Auftragsart wird nur noch bis zum 31.12.2004 unterstützt.

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Kennung	Text	Satzlänge ⁹	Bits	Format
EIB	Ausführungsanzeige (Exportinkasso) Bank an Kunde abholen	-1	7	EDIFACT
EIK	Senden Exportinkassi	-1	7	EDIFACT
ESA	EDIFACT senden ASCII	-1	7	EDIFACT
ESM ¹¹	EU-Standardüberweisung (Zahlungsart 13) im Magnetbandformat (Satzlängen- feld 4 Bytes)	64	8	DTAZV-Magnetband
ESR	Einreichung von EDIFACT-Lastschriften	-1	7	EDIFACT
ESZ	EDIFACT senden EBCDIC	-1	8	EDIFACT
ESU ¹²	EU-Standardüberweisung (Zahlungsart 13)	256	7	DTAZV
EUE	Taggleiche grenzüberschreitende Euro-Eilzahlung	256	7	DTAZV
GAB	Abholen Garantien	-1	7	MT760, MT767
GAK	Senden Garantien	-1	7	MT760
GKT	GeldKarte-Umsatz senden (Datenauf- bau gemäß GeldKarte-Spezifikation)	128	7	DTAUS
IDD	Internationale Lastschriften	-1	7	MT104
IIB	Abholen Importinkassi	-1	7	MT410 – 419
IIK	Senden Importinkassi	-1	7	MT410 – 419
INT	Internationaler Zahlungsverkehr	-1	7	MT100 ¹³ , MT101, MT104
IZG	Inlandszahlungsverkehrsauftrag senden (nur Gutschriften)	128	7	DTAUS0
IZL	Inlandszahlungsverkehrsauftrag senden (nur Lastschriften)	128	7	DTAUS0
IZV	Inlandszahlungsverkehrsauftrag sen- den	128	7	DTAUS0
MAO	Abholen Magnetband-Datei aus optischer Beleglesung	-1	7	MAOBE
MCV	Senden IZV-Magnetbandformat (Satzlängenfeld 4 Bytes)	64	8	DTAUS-Magnetband
MC2	Senden IZV-Magnetbandformat (Satzlängenfeld 2 Bytes)	64	8	DTAUS-Magnetband
MC4	Senden IZV-Magnetbandformat (Satzlänge variabel)	-1	8	DTAUS-Magnetband
POZ	Senden POZ-Datei	128	7	DTAUS0
RDT	Rücklastschrift an Kunde	128	7	DTAUS0
RFT	Request for Transfer	-1	7	MT101

¹¹ Soweit die separate Einlieferung von EU-Standardüberweisungen im Magnetbandformat vereinbart wurde, ist diese Auftragsart zu verwenden.

¹² Soweit die separate Einlieferung von EU-Standardüberweisungen vereinbart wurde, ist diese Auftragsart zu verwenden (außer Magnetbandformat, dann ist ESM zu verwenden).

¹³ Der MT100 kann nur noch bis zum 15.11.2003 verwendet werden.

Kennung	Text	Satzlänge ⁹	Bits	Format
STA	Abholen Swift-Tagesauszüge	-1	7	MT940
VMK	Abholen kurzfristige Vormerkposten	-1	7	MT942
VML ¹⁴	Abholen langfristige Vormerkposten	-1	7	MT942
WPA	Abholen Wertpapierabrechnung	-1	7	MT510, MT515
WPB	Abholen Wertpapierausführungsanzeige	-1	7	MT519, MT513
WPC	Abholen Depotaufstellung	-1	7	MT571, MT535
WPD	Abholen sonstige WP-Umsätze	-1	7	MT572, MT536

1.4.2 Kategorie 2: Systembedingte Auftragsarten

Kennung	Text	Satzlänge ¹⁵	Bits	Format
BPD	Bankparameterdatei abholen (automatische Abholung durch das Kundenprodukt)	-1	8	
INI	Passwort-Initialisierung	512	8	Public Key des Kunden für die EU; siehe Anlage 2 (Standards für die Sicherheit)
PTK	Abholen Kundenprotokoll	-1	7	siehe 1.7 „Kundenprotokoll - inhaltliche und formale Festlegungen“
PUB	Senden Public Key zur Unterschriftenverifizierung	512	8	Public Key des Kunden für die EU; siehe Anlage 2 (Standards für die Sicherheit)
PWA	Passwort-Änderung senden	1	7	Übertragung einer Dummy-Datei, die nur ein Leerzeichen enthält
SPR	Sperren der Zugangsberechtigung	1	7	Übertragung einer Dummy-Datei, die nur ein Leerzeichen enthält
VPB	Abholen Public Key der Bank zur Verschlüsselung	512	8	Public Key der Bank zur Verschlüsselung (siehe Anlage 2, Kapitel 2.3.3 „Vorbereitung der Verschlüsselung / Public-Key-Austausch“)

¹⁴ Diese Auftragsart wird nur noch bis zum 31.12.2004 unterstützt.

¹⁵ Die Satzlänge „-1“ bedeutet „variable Satzlänge“.

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Kennung	Text	Satzlänge ¹⁵	Bits	Format
VPK	Senden Public Key des Kunden zur Verschlüsselung	512	8	Public Key (siehe Anlage 2, Kapitel 2.3.3 „Vorbereitung der Verschlüsselung / Public-Key-Austausch“)

1.4.3 Kategorie 3: Reservierte Auftragsarten für den zwischenbetrieblichen Zahlungsverkehr/Dateiaustausch

Kennung	Text	Satzlänge ¹⁶	Bits	Format
FIN	EDIFACT-FINPAY senden	-1	7	EDIFACT
IZS	Informationen von Zentralstellen	80	7	
SSP	ec-Karten-Sperrdatei	80	8	

1.4.4 Kategorie 4: Sonstige reservierte Auftragsarten unter Verwendung nicht standardisierter Formate und Verfahren

Kennung	Text	Satzlänge ¹⁶	Bits	Format
ATA	Teilausnutzung Importakkreditiv (Kreditinstitut an Kunde)	-1	7	
BAK ¹⁷	Auftragsart für elektronische Kontoauszüge	-1	8	
BZK	Barzahlungskarte			
DKI	Devisenkursinformationen abholen (Euro)	-1	8	
DMI	Abholen Devisenmarktinformationen	-1	7	
DSW	Abholen Devisenswapinformationen	-1	7	
ESG	ESG-Datei für Elektronische Zweitunterschrift abholen	-1	8	
ESP	ESP-Datei für Elektronische Zweitunterschrift senden	-1	8	
FTB	Abholen beliebige Datei	-1	8	General-stream ASCII
FTB	Senden beliebige Datei	-1	8	General-stream ASCII
FTD	Freie Textdatei senden	-1	7	ASCII

¹⁶ Die Satzlänge „-1“ bedeutet „variable Satzlänge“.

¹⁷ Die Anforderungen (Geschäftsprozesse, Formate) an einen steuerrechtlich anerkannten elektronischen Kontoauszug sind noch nicht definiert.

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Kennung	Text	Satzlänge ¹⁶	Bits	Format
FTD	Freie Textdatei abholen	-1	7	ASCII
IBK	Abholen Institutsbestätigungsdatei Komplettbestand	-1	8	
IBW	Abholen Institutsbestätigungsdatei Komplettbestand weitere Datei	-1	8	
IBU	Abholen Institutsbestätigungsdatei tägliches Update	-1	8	
IKK	Senden Institutskonten Komplettbe- stand begrenzt auf 170 MB	-1	8	
IKU	Senden Institutskonten tägliches Up- date	-1	8	
IKW	Senden Institutskonten Komplettbe- stand weitere Datei	-1	8	
KTH	KTOHIN Automatisiertes Verfahren für die Ände- rung von Kontonummern und Bankleit- zahlen	100	8	EBCDIC
KTR	KTORUECK Automatisiertes Verfahren für die Ände- rung von Kontonummern und Bankleit- zahlen	100	8	EBCDIC
KKZ	Kontenkonzentration und Saldenaus- gleich			
TST	Senden Testdatei ASCII	-1	7	ASCII
TST	Abholen Testdatei ASCII	-1	7	ASCII
UPD	Updates abholen ¹⁸	-1	8	

¹⁸ Bereitstellung von Updates durch das Kreditinstitut und Abholung durch das Kundensystem, signalisiert durch die Auftragsart UPD.

1.5 Fehlermeldungen/Fehlercodes

Beschreibung der Ursache für die Ablehnung des Transfer-Auftrages oder Quittung auf Aufträge, die keinen File-Transfer erfordern (z. B. INI, PWA) (maximal 120 Bytes alphanumerisch).

Aufbau:

- Byte 1 – 40: freier Fehlertext (zur Anzeige am PC)
- Byte 41 – 44: Fehlercode
- Byte 45 – 120: nicht normiert

Zur Zeit sind folgende Fehlercodes definiert:

Nummer	Bedeutung
1	Auftrag durchgeführt (Spezifizierung des Auftrags erfolgt im Fehlertext)
2	User-ID nicht registriert
3	Falsches Passwort
5	User-ID gesperrt
7	Unzulässige Auftragsart
8	User-ID nicht initialisiert
13	(noch) keine Daten vorhanden; später versuchen
15	Keine Berechtigung für diese Auftragsart
16	Formalfehler
17	Sperrung der User-ID nach 3 Fehlversuchen
24	Keine Daten vorhanden
25	User-ID noch nicht freigegeben
26	Nicht normierter Fehler, Wiederholung nicht sinnvoll
27	Nicht normierter Fehler, Wiederholung sinnvoll
29	Abbruch der gesamten DFÜ-Verbindung

1.6 Betrieb über asynchrone Verbindungen und PAD

Die Spezifikation behandelt das Verfahren zur Erkennung und Beseitigung von Datenverfälschungen bei Datenübertragungen über Telefonverbindungen.

Es werden die Protokollelemente und der Ablauf spezifiziert, weiterhin die Konfigurationsparameter und die Formate der Kontroll- und Dateneinheiten erläutert. Außerdem sind die benötigten Algorithmen zur Erkennung von Datenverfälschungen spezifiziert.

1.6.1 Anforderungen an das Verfahren

- Der Kommunikationsweg geht vom Modem über X.28/X.29-Protokoll zu einem PAD (in-house oder öffentlich) und von diesem PAD über eine normale X.25-Verbindung zum Partner.
- Es wird ein Verfahren spezifiziert, das unterhalb der OSI-Transportschicht arbeitet.
- Es besteht die Notwendigkeit, Datenübertragungen über Strecken, die nur einen 7-bit Zeichensatz unterstützen, zu realisieren. Außerdem sollten Zeichen, die eventuell eine Bedeutung als PAD-Steuerzeichen haben, nicht direkt übertragen werden.
- Da die höheren Protokolle (FTAM) 8-bit-Zeichen benötigen, wird ebenfalls unterhalb der Transportschicht ein Mechanismus zur Maskierung/Demaskierung der nicht übertragbaren Zeichen spezifiziert.

1.6.2 Kurzbeschreibung der Lösung

Prinzipiell kann bei unsicheren Verbindungen folgendermaßen gearbeitet werden:

- Zu übertragende Daten werden mit einer Checksumme gesichert. Auf der Empfangsseite muss die Checksumme gegengerechnet werden, und Quittungen benachrichtigen den Sender, ob die Übertragung erfolgreich war oder nicht.
- Da auch Quittungen verfälscht werden können, muss der Sender das Eintreffen von Quittungen durch Timer überwachen.
- Das Sicherungsverfahren selbst ist als eigendefinierte Protokollschicht zwischen der OSI-Transportschicht und der Netzwerkschicht angesiedelt. Das Verfahren versendet eigene Kontroll- und Dateneinheiten, in denen die Übertragungseinheiten der Transportschicht (TPDU) als Netzwerkdaten (NSDU) codiert sind.
- Umgekehrt empfängt das Verfahren Daten der Netzwerkschicht (NSDU), überprüft sie auf Korrektheit und behandelt sie als Elemente des eigenen Protokolls. Der Inhalt der Dateneinheiten wird decodiert und in dieser Form als TPDU an die Transportschicht hochgereicht.

1.6.3 Spezifikation

1.6.3.1 Kontroll- und Dateneinheiten

Folgende Einheiten (NSDU) werden spezifiziert:

- Austausch von Steuerparametern
 - CONNECT Mitteilung über gewünschte Steuerparameter durch den Initiator der Netzwerkverbindung
 - ACCEPT Bestätigung oder Modifizierung der Steuerparameter durch den passiven Partner.

- Datenaustausch

DATA	Enthält in codierter Form sowohl Transport-Steuer-PDU als auch Transport-Daten-PDUs.
------	--

- Quittungen

ACK	Positive Quittung für eine DATA NSDU.
-----	---------------------------------------

NAK	Negative Quittung für eine DATA NSDU
-----	--------------------------------------

1.6.3.2 Protokollabläufe

Grundsätzlicher Ablauf:

- Nach Aufbau der Netzwerkverbindung sendet der Initiator eine CONNECT-NSDU, in der der Initiator dem Partner mitteilt, welche Protokollversion und welchen Übertragungsmodus (7-bit oder 8-bit) er benutzen will.
- Der Partner sendet nach Empfang der CONNECT-NSDU eine ACCEPT-NSDU, in der der Partner die vorgeschlagenen Steuerparameter bestätigt oder modifiziert (vergleiche 1.6.3.5 Datenformate der Kontroll- und Dateieinheiten, CONNECT und ACCEPT). CONNECT- und ACCEPT-NSDUs werden grundsätzlich nur einmal zu Beginn der Netzdatenphase ausgetauscht. Es ist jedoch möglich, dass die NSDUs verfälscht werden. Aus diesem Grund überwacht der Initiator den Empfang der ACCEPT-NSDU mit einem Timer, um die CONNECT-NSDU gegebenenfalls erneut zu versenden. Der Partner muss zu Beginn der Datenphase mehrere CONNECT-NSDUs empfangen können und er muss diese jeweils durch eine ACCEPT-NSDU bestätigen können.
- Erst nach Austausch der CONNECT- und ACCEPT-NSDU können Daten- und Quittungs-NSDUs gesendet werden.
- Das Quittungsverfahren für empfangene DATA-NSDUs gestaltet sich wie folgt:
Der Empfänger quittiert sofort jede empfangene DATA-NSDU
-- bei Korrektheit der Daten mit einer ACK-NSDU
-- bei verfälschten Daten mit einer NAK-NSDU.

Erhält der Sender eine NAK-NSDU, so wiederholt der Sender die zuletzt gesendete DATA-NSDU.

Da auch Quittungen verfälscht sein können, muss der Sender die zuletzt gesendete DATA-NSDU wiederholen, wenn nach einer bestimmten Zeitspanne keine Quittung eingetroffen ist. Umgekehrt muss der Empfänger doppelt empfangene Daten zwar positiv bestätigen, sie ansonsten aber ignorieren.

1.6.3.3 Mögliche Abläufe beim Austausch von Dateneinheiten

A und B bezeichnen die beiden beteiligten Kommunikationsinstanzen, die Zeit läuft von oben nach unten. Die Zahlen bedeuten eine Durchnummerierung der Einheiten.

Mit Fehler ist im Folgenden gemeint, dass eine der folgenden Bedingungen zutrifft:

- Eine NSDU verstößt gegen das spezifizierte NSDU-Format.

- Die Länge einer NSDU ist falsch.
- Der Typ einer NSDU kann nicht erkannt werden.
- Ein Sequenzfehler wurde erkannt.
- Bei der Gegenrechnung der Checksumme wird ein Fehler erkannt.

Beispiel 1 (Normalfall): Die Übertragung von A nach B und die Übertragung der Quittung ist erfolgreich. Wenn vorhanden, kann A mit der Übertragung der nächsten DATA-NSDU fortfahren.

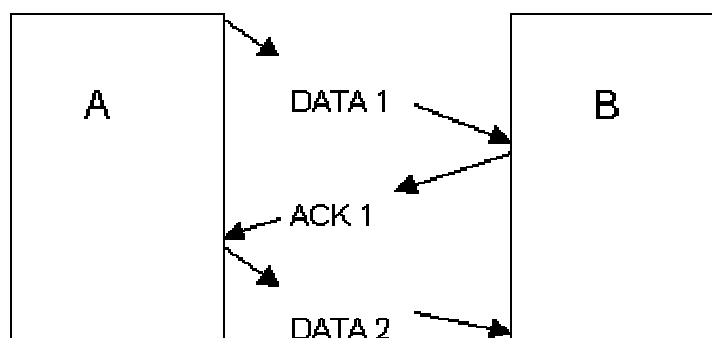


Abbildung 1.3 Mögliche Abläufe beim Austausch von Dateneinheiten – Beispiel 1

Das ist der Normalfall. Die Übertragung von A nach B und die Übertragung der Quittung ist erfolgreich. Wenn vorhanden, kann A mit der Übertragung der nächsten DATA-NSDU fortfahren.

Beispiel 2 (B erkennt Fehler in den von A gesendeten Daten): B erkennt einen Fehler in den von A gesendeten Daten und schickt eine negative Quittung. A muss dieselbe NSDU noch einmal versenden.

Unter Umständen interpretiert der Empfänger eine verfälschte Kontroll-NSDU (CONNECT, ACCEPT, ACK oder NAK) als Daten-NSDU und sendet ein NAK mit einer Sequenznummer (BSN = Block Sequence Number), die noch gar nicht verschickt wurde. Ein solches NAK muss vom Sender ignoriert werden.

Randbedingungen, wie z. B. maximale Anzahl der Versuche, sind in Kapitel 1.6.3.4 Konfigurationsparameter spezifiziert.

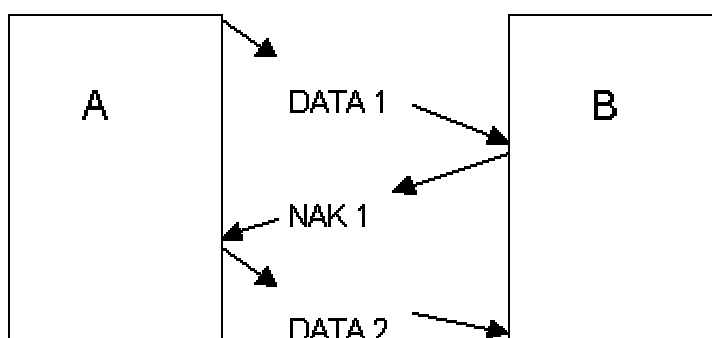


Abbildung 1.4 Mögliche Abläufe beim Austausch von Dateneinheiten – Beispiel 2

Beispiel 3 (Daten erreichen B nicht oder sind nicht als solche zu erkennen): A schickt Daten, bei B kommt überhaupt nichts an, bzw. die Daten sind so verfälscht, dass sie nicht als solche erkannt werden können. In diesem Fall läuft der Quittungsüberwachungstimer bei A ab, und A sendet die NSDU erneut.

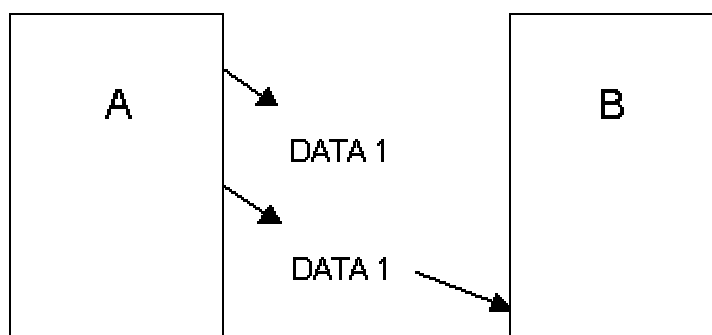


Abbildung 1.5 Mögliche Abläufe beim Austausch von Dateneinheiten – Beispiel 3

Beispiel 4 (Quittung von B erreicht A nicht): A schickt Daten, die von B (positiv oder negativ) quittiert werden. Beim Empfang der Quittung wird entweder ein Fehler erkannt, oder die Quittung wird überhaupt nicht empfangen. In diesem Fall läuft der Quittungsüberwachungstimer bei A ab, und dieselbe NSDU wird noch einmal gesendet.

Aus diesem Fall folgt, dass B erkennen muss, wenn zweimal hintereinander dieselbe NSDU empfangen wird. Die Kopie kann einfach vernichtet werden, muss aber quittiert werden.

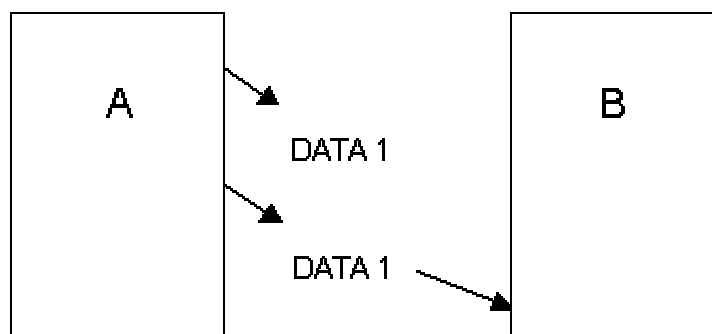


Abbildung 1.6 Mögliche Abläufe beim Austausch von Dateneinheiten – Beispiel 4

Protokollverstöße: Folgendes gilt als Protokollverstoß und führt zum Abbau der Verbindung:

- wenn NSDUs des Datenaustauschs (DATA, ACK, NAK) empfangen werden, bevor CONNECT- und ACCEPT-NSDUs ausgetauscht worden sind
- wenn CONNECT- oder ACCEPT-NSDUs empfangen werden, nachdem bereits Dateneinheiten empfangen wurden, so
- wenn Daten mit falscher Sequenznummer empfangen werden (Quittungen mit falscher Sequenznummer werden jedoch ignoriert).

1.6.3.4 Konfigurationsparameter

Die folgende Tabelle beschreibt die variabel konfigurierbaren Parameter für die lokale Instanz der beschriebenen Protokollschicht.

Parameter	Default	Bedeutung
BCS_ACK_TIMEOUT	5	Zeitspanne (in Sekunden), nach der eine Quittung empfangen worden sein muss. Nach Ablauf dieser Zeitspanne muss die unquitierte DATA-NSDU oder die unbestätigte CONNECT-NSDU wiederholt werden.
BCS_N_MAX_REP	5	Maximale Anzahl der Übertragungsversuche für eine NSDU. Ist die maximale Anzahl der Wiederholversuche überschritten, wird die Verbindung abgebaut. In diesem Fall sorgt die FTAM Recovery-Prozedur für den Wiederanlauf der Datenübertragung.
BCS_G_MAX_REP	30	Maximale Anzahl der Wiederholungen für eine gesamte Verbindung. Ist die maximale Anzahl der Wiederholversuche überschritten, wird die Verbindung abgebaut. In diesem Fall sorgt die FTAM Recovery-Prozedur für den Wiederanlauf der Datenübertragung.
BCS_MODE	8	Bestimmt, ob die Übertragungsstrecke im 7-bit- oder 8-bit-Modus arbeitet.

Die Werte können über Environmentvariablen (Umgebungsvariablen) eingestellt werden. Für eine nicht gesetzte Environmentvariable wird automatisch der Default-Wert angenommen.

1.6.3.5 Datenformate der Kontroll- und Dateieinheiten

Dieses Kapitel beschreibt die Formate der Einheiten (NSDU), die nach dem Protokoll (vgl. vorausgegangene Kapitel) ausgetauscht werden.

Der Aufbau einer NSDU richtet sich nach dem allgemeinen Schema:

Anzahl Bytes	1	1	1	n	2	1
	SOH	type	BSN	Daten	BCS	CR

Bezeichnung	Bedeutung / Wert
SOH	Damit beginnt eine neue NSDU, SOH hat den Wert 0x01.

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Bezeichnung	Bedeutung / Wert
Type	Bestimmt den Typ einer NSDU
BSN	Sequenznummer der NSDU. Der Wert läuft numerisch zwischen 0 und 9 und wird als ASCII-Codierung der Zahl übertragen (bei den CONNECT- und ACCEPT-NSDUs wird kein BSN verwendet).
Daten	<i>Bei Data-NSDUs:</i> Zu übertragende Daten (codierte TPDUs). <i>Bei CONNECT- und ACCEPT-NSDUs</i> Steuerparameter (siehe Beschreibung von CONNECT und ACCEPT in diesem Kapitel) <i>Bei ACK- und NAK-NSDUs</i> Quittungs-NSDUs haben keinen Datenteil.
BCS	Checksumme (vgl. Beschreibung des Algorithmus in Kapitel 1.6.3.6 „Berechnung der Checksumme und Codierung der NSDU im 7- oder 8-bit Modus“)
CR	Beendet immer eine NSDU. CR hat den Wert 0x0d.

Die Codierung der Typenfelder erfolgt durch weit auseinanderliegende Bitmuster, um ein Verwechseln der Typen durch einzeln umkippende Bits unwahrscheinlich zu machen.

CONNECT:

Diese NSDU wird vom Initiator direkt nach Aufbau der Netzverbindung gesendet.

Anzahl Bytes	1	1	1	1	1	2	1
	SOH	0x20	version	window	bitmode	BCS	CR

Bezeichnung	Bedeutung	Wert
version	Gibt die Version des Sicherungsverfahrens des Initiators an	(zur Zeit): 0x31
window	Sendefenster des Initiators	immer 0x31
bitmode	Gibt an, ob der Initiator den 7- oder 8-bit Übertragungsmodus vorschlägt	0x31 oder 0x38

ACCEPT:

Diese NSDU wird vom Responder nach Empfang der CONNECT-NSDU gesendet.

Anzahl Bytes	1	1	1	1	1	1	2	1
	SOH	0x23	result	version	window	bitmode	BCS	CR

Bezeichnung	Bedeutung	Wert
result	Gibt an, ob der Responder die Verbindung annimmt	0x20: Aufbau OK sonst: Fehler, noch nicht spezifiziert
version	Gibt die Version des Sicherungsverfahrens des Responders an	(zur Zeit): 0x31
window	Sendefenster des Responders	immer 0x31

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Bezeichnung	Bedeutung	Wert
bitmode	Gibt an, ob der Responder den 7- oder 8-bit Übertragungsmodus wählt	0X31 oder 0X38

Die Parameter version und bitmode werden ausgehandelt, d. h. der Responder kann kleinere Werte setzen, als der Initiator vorgeschlagen hat. Das bedeutet, version auf eine ältere Version und/oder bitmode von 8 auf 7 herunterzuhandeln.

Die in der ACCEPT-NSDU angegebenen Werte für version und bitmode bestimmen damit das Sicherungsverfahren für die Dauer der Verbindung.

DATA:

Anzahl Bytes	1	1	1	n	2	1
	SOH	0x40	BSN	Daten	BCS	CR

Bezeichnung	Bedeutung	Wert
BSN	beinhaltet die Sequenznummer dieser NSDU	0X30 bis 0X39 (siehe Beschreibung der BSN im allgemeinen NSDU-Schema, s.o.)

ACK:

Anzahl Bytes	1	1	1	2	1
	SOH	0x71	BSN	BCS	CR

Bezeichnung	Bedeutung	Wert
BSN	beinhaltet die Blocknummer der nächsten erwarteten DATA-NSDU	0x30 bis 0x39 (siehe Beschreibung der BSN im allgemeinen NSDU-Schema, s.o.)

NAK:

Anzahl Bytes	1	1	1	2	1
	SOH	0x7f	BSN	BCS	CR

Bezeichnung	Bedeutung	Wert
BSN	beinhaltet die Blocknummer der nächsten erwarteten DATA-NSDU	0x30 bis 0x39 (siehe Beschreibung der BSN im allgemeinen NSDU-Schema, s.o.)

1.6.3.6 Berechnung der Checksumme und Codierung der NSDU im 7- oder 8-bit Modus

Dieses Kapitel beschreibt die Codierung einer NSDU, also auch den Übergang von Daten einer TPDU zu Daten einer NSDU. Der Vorgang beinhaltet folgende Schritte:

- Erstelle SOH
- Berechne BCS
- Maskiere verbotene Zeichen (Shift-Out- bzw. Shift-In-Logik)
- Erstelle BCS und CR.

Algorithmus zur Berechnung der BCS:

Der Algorithmus zur Berechnung der BCS folgt dem ISO TRANSPORT LAYER Standard.

Verwendete Symbole	Bedeutung / Wert
CO, C1	Variablen, die im Algorithmus benötigt werden
X	Wert des ersten Bytes der BCS
Y	Wert des zweiten Bytes der BCS
N	Anzahl der zu versendenden Bytes ohne SOH und CR

Der Algorithmus beinhaltet folgende Schritte:

- Initialisieren von CO und C1 mit Null.
- Bearbeiten jedes Bytes von $i = 1$ bis n mit:
 - Addieren des Byte-Wertes zu CO und anschließend
 - Addieren des Wertes von CO zu C1.
- Berechnen von X und Y mit
$$X = CO - C1$$
$$Y = C1 - 2 * CO$$
- Speichern der Werte X und Y in den Bytes 1 und 2 der BCS.

Algorithmus zur Maskierung der Zeichen (Sender):

Verwendete Symbole	Wert
SO	0X0e
SI	0X0f
n	Anzahl der zu versendenden Bytes, einschließlich BCS, jedoch ohne SOH und CR

```
for (i = 1 to n) {
  x = buffer [i];
  if ((7 < bit_mode) && (0x80 <= x)) {
    x = x & 0x7f;
    if {x < 0x20} {
      output (SO);
      output (x + 0x40);
    } else {
      output (SI);
      output (x);
    }
  } else {
    if ((x & 0x7f) < 0x20) {
      output (SO);
      output (x + 0x20);
    }
    else {
      output (x);
    }
  }
}
```

Abbildung 1.7 Der Algorithmus zur Maskierung

Anmerkung: Unabhängig vom gewünschten Übertragungsmodus muss die CONNECT-NSDU immer im 7-bit-Modus codiert sein.

1.6.3.7 Decodierung und Prüfung der NSDU

Eine empfangene NSDU wird in folgenden Schritten bearbeitet:

- Prüfe das Format der NSDU
- Demaskiere verbotene Zeichen (Shift-Out- bzw. Shift-In-Logik)
- Prüfe BCS
- Entferne SOH, BCS und CR.

Algorithmus zur Prüfung der BCS:

Der Algorithmus zur Prüfung der BCS folgt dem ISO TRANSPORT LAYER Standard.

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Verwendete Symbole	Wert
CO, C1	Variablen, die im Algorithmus benötigt werden
n	Anzahl der zu demaskierenden Bytes einer empfangenden NSDU, einschließlich BCS, jedoch ohne SOH und CR

Der Algorithmus beinhaltet folgende Schritte:

- Initialisieren von CO und C1 mit Null.
- Bearbeiten jedes Bytes von $i = 1$ bis n mit
 - Addieren des Byte-Wertes zu CO und anschließend
 - Addieren des Wertes von CO zu C1.
- Wenn alle Bytes (einschließlich BCS) bearbeitet sind und einer oder beide Werte von CO und C1 nicht Null sind, liegt ein Checksummenfehler vor.

Es liegt in der Natur des Algorithmus, dass es nicht notwendig ist, explizit die gespeicherten Bytes der Checksumme zu vergleichen.

Algorithmus zur Demaskierung der Zeichen (Empfänger):

Verwendete Symbole	Wert
SO	0X0e
SI	0X0f
n	Anzahl der zu versendenden Bytes, einschließlich BCS, jedoch ohne SOH und CR


```
for (i = 1 to n) {
  x = buffer [i];
  if (x < 0x20) {
    switch (x) {
      case S0:
        i = i + 1;
        y = buffer [i];
        if ((y>=0x20) && (y<0x40) || ((y>=0xa0) && (y<0xc0)))
          output (y - 0x20);
        else {
          if ((y >= 0x40) && (y < 0x60))
            output ((y - 0x40) I 0x80);
          else
            error();
        }
        break;
      case SI:
        i = i + 1;
        y = buffer [i];
        if ((y >= 0x20) && (y < 0x80))
          output (y I 0x80);
        else
          error();
        break;
      default:
        error();
        break;
    }
  } else {
    if ((x >= 0x80) && (x < 0xa0))
      error();
    else
      output (x);
  }
}
```

Abbildung 1.8 Der Algorithmus zur Demaskierung

1.6.4 Abkürzungsverzeichnis

- ACK Acknowledge
- BCS Block CheckSum (Checksumme)
- BSN Block Sequence Number (Sequenznummer)
- CR Carriage Return
- FTAM File Transfer Access and Management
- NAK Negative Acknowledge
- NSDU Network Layer Service Data Unit
- OSI Open Systems Interconnection
- PAD Packet Assembler Disassembler
- PC Personal Computer
- PDU Protocol Data Unit
- TPDU Transport Protocol Data Unit
- SI Shift-In
- SO Shift-Out
- SOH Start of Header

1.7 Kundenprotokoll - inhaltliche und formale Festlegungen

Das Kundenprotokoll ist auf der Bankseite gemäß den folgenden Festlegungen zu erstellen. Es gelten hierbei folgende grundsätzliche Bestimmungen:

- Es dürfen in einer Zeile maximal 72 Zeichen ausgegeben werden.
- Es erfolgt kein Protokolleintrag über die Weiterverarbeitung. (Ausnahmen: EU-Prüfung, Fehler bei Dekomprimierung, Anzeige Dateinhalt)
- Der A- und E-Satz (bei Dateien im DTAUS-Format, z. B. IZV-Dateien), der Q-Satz und Z-Satz (bei Dateien im DTAZV-Format, z. B. AZV-Dateien) und der erste und letzte logische Satz (bei allen anderen Dateitypen) wird auch bei Dateien ohne EU ausgegeben.

1.7.1 Inhaltliche Festlegungen

Dateiname des Kundenprotokolls:

Als Dateiname wird die jeweilige Kunden-ID mit der Extension „PTK“ verwendet:

<KUNDEN-ID>.PTK

Auflistung der einzelnen Datenfelder je Aktion auf der Bankseite:

Je Aktion auf der Bankseite sind folgende Daten im Kundenprotokoll zu dokumentieren:

Zu dokumentierende Daten	Beschreibung
Datum und Uhrzeit	Datum und Uhrzeit der Aktion auf dem Banksystem
Art der Aktion	Siehe Kap. 1.7.3 Liste der möglichen Meldungen inklusive Textnummer
Hostname	
Auftragsart	Klartext zu der vom Kunden benutzten Auftragsart, auf die sich die jeweilige Aktion der Bank bezieht. Beispiel: „Freie Textdatei im 7 Bit-Code senden“; siehe Kapitel 1.4 „Auftragsartenkennungen“

Folgende Felder sind bei EU-Prüfung gegebenenfalls mehrfach (d. h. je User) vorhanden:

- User-ID
- User-Name (nur soweit vorhanden)
- Auftragsnummer
(Byte 23 bis 26 aus dem Remote-Filename; siehe Kapitel 1.1. „Anwendungsprotokoll Kunden-/Bankrechner“)
- Ergebnis der Aktion (siehe Kapitel 1.7.3 „Liste der möglichen Meldungen inklusive Textnummer“)

Folgende Einträge sind (mit Ausnahme der Dateianzeige) nur bei EU-Prüfungen vorhanden:

Eintrag	Beschreibung
Dateiname auf Kundensystem	„Dateiname der Originaldatei“ aus EU-Datei; siehe Kapitel 2.2.2.5 „Formate“ (Anlage 2 (Standards für die Sicherheit))
Dateianzeige	Auftragsarten (Dateien im DTAUS-Format): Anzeige der wesentlichen Dateidaten ¹⁹ entsprechend dem Inhalt der Datenträgerbegleitzettel; siehe Kapitel 1.7.4 „Dateianzeige auf Kunden- und Bankseite“ Sonstige Auftragsarten ²⁰ : Bei <u>Dateien mit fester Satzlänge</u> wird der erste und letzte Satz gemäß der je Auftragsart spezifizierten Satzlänge angezeigt. Bei <u>Dateien mit variabler Satzlänge</u> wird der erste und letzte logische Satz angezeigt (Satz vor dem ersten CR/LF, Satz vor dem letzten CR/LF).
Erläuternder Text im Fehlerfall	Dieses Feld wird nur angezeigt, wenn das Ergebnis der Aktion „EU-Prüfung“ einen Fehler anzeigt. Es ist damit als Subfeld hierzu zu verstehen, das den konkreten Fehlerfall (gegebenenfalls je User und je logischer Datei) erläutert; Beispiel: „Vereinbarter Höchstbetrag ueberschritten“, siehe Kapitel 1.7.3 „Liste der möglichen Meldungen inklusive Textnummer“.

1.7.2 Formale Festlegungen

Die formale Gestaltung des Kundenprotokolls erfolgt gemäß folgenden Festlegungen:

1.7.2.1 Protokollierung der Aktionen auf der Bankseite

1. Zeile:

- Datum (tt.mm.jj)
- 1 Leerzeichen
- Uhrzeit (hh:mm:ss)
- 5 Leerzeichen
- Art der Aktion (maximal 50 Zeichen)

¹⁹ Bei „Sammel-EU“ (mehrere logische Dateien mit einer EU) erfolgt die Anzeige je logischer Datei

²⁰ Bei 8-Bit-Dateien wird der erste und letzte Satz als HEXDUMP ausgegeben.

Beispiel:

14.11.02 11:39:05	Datei zur Bank uebertragen
-------------------	----------------------------

3. Zeile:

- 9 Leerzeichen Einrückung (aus Übersichtlichkeitsgründen)
- Text: „Auftrag“ (= Art des Protokolleintrags)
- 4 Leerzeichen
- Doppelpunkt (dieses Zeichen steht immer an der 21. Stelle)
- 1 Leerzeichen
- Text der Auftragsart (42 Zeichen, ggf. mit Leerzeichen aufgefüllt)
- Auftragsartenkennung (3stellig)
- 1 Leerzeichen
- Auftragsnummer (4stellig)

Beispiel:

Auftrag	: Freie Textdatei im 7Bit-Code senden	FTD A000
---------	---------------------------------------	----------

Sonstige Zeilen:

- 9 Leerzeichen Einrückung
- Art des Protokolleintrags (maximal 11 Zeichen)
- Doppelpunkt (dieses Zeichen steht immer an der 21. Stelle)
- 1 Leerzeichen
- Text des jeweiligen Protokolleintrages (maximal 50 Zeichen)

Beispiele:

Hostname	: BVFTAMU
----------	-----------

Ergebnis	: Uebertragung in Ordnung Datenuebertragung unverschlusselt Datenübertragung unkomprimiert
----------	--

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Durch Anfügen zweier zusätzlicher Textzeilen an die Ergebniszeile wird dokumentiert, dass die DFÜ-Aufträge ohne bzw. mit Verschlüsselung und Komprimierung abgewickelt wurden. Die erste zusätzliche Zeile dokumentiert die Verschlüsselung, die zweite Zeile die Komprimierung des DFÜ-Auftrages.

1. Zeile:

- 22 Leerzeichen Einrückung
- Text: „Datenuebertragung verschluesselt“ oder „Datenuebertragung unverschluesselt“

2. Zeile:

- 22 Leerzeichen Einrückung
- Text „Datenuebertragung komprimiert“ oder „Datenuebertragung unkomprimiert“

Beispiele für die Protokollierung gesamt:

```
14.11.02 11:40:05      Datei zur Bank uebertragen
      Hostname       : HOSTFTAM
      Auftrag        : Beliebige Datei senden                      FTB AAI0
      Teilnehmer      : USER Teilnehmer User
      Ergebnis       : Uebertragung in Ordnung
                     Datenuebertragung unverschluesselt
                     Datenuebertragung unkomprimiert
```

```
14.11.02 11:44:15      Datei zur Bank uebertragen
      Hostname       : HOSTFTAM
      Auftrag        : Beliebige Datei senden                      FTB AAJ0
      Teilnehmer      : USER Teilnehmer User
      Ergebnis       : Uebertragung in Ordnung
                     Datenuebertragung verschluesselt
                     Datenuebertragung komprimiert
```

1.7.2.2 Protokollierung der Fehler bei Unterschriftsprüfung

Teilnehmerbezogene Fehler bei Unterschriftsprüfung:

- 9 Leerzeichen Einrückung
- Text: „EU von“
- 1 Leerzeichen
- USER-ID (maximal 8 Zeichen)
- Doppelpunkt (dieses Zeichen steht an der 26. Stelle)

- 1 Leerzeichen
- Fehlertext (maximal 45 Zeichen)

Beispiel:

EU von BLUMPC : Vereinbarter Hoechstbetrag ueberschritten

Allgemeine Fehlertexte bei Unterschriftsprüfung:

- 9 Leerzeichen Einrückung
- Fehlertext (maximal 63 Zeichen)

Beispiel:

Die erforderliche Anzahl von EUs ist nicht vorhanden

1.7.2.3 Dateianzeige

- 4 Leerzeichen Einrückung
- Dateianzeige

Beispiel siehe 1.7.4 Dateianzeige auf Kunden- und Bankseite

1.7.2.4 Unterstützung fremdsprachiger Kundenprotokolle

Das Kundenprotokoll kann nicht nur in deutscher Sprache, sondern auch optional in anderen Sprachen generiert werden.

In diesem Zusammenhang ist zu beachten, dass im Protokoll enthaltene Informationen, die nach Abholung auf der Kundenseite maschinell ausgewertet werden (z. B. Ergebnisse der EU-Prüfungen), gesondert gekennzeichnet werden müssen. Auf diese Weise kann gewährleistet werden, dass die maschinelle Auswertung der in verschiedenen Sprachen erzeugten Protokolle in der Kundensoftware funktioniert.

Zu diesem Zweck werden alle Informationen, die für eine maschinelle Auswertung von Bedeutung sind, durch Anfügen einer eindeutigen, 2stelligen Nummer gekennzeichnet. Der eigentliche Text wird von der eindeutigen Nummer durch ein Leerzeichen getrennt. Die Nummer wird durch Klammern „[]“ begrenzt.

Nach Durchführung eines Protokollabrufes können die eindeutigen Nummern dann durch das Kundensystem im Rahmen der maschinellen Auswertung unabhängig von der jeweiligen Sprache entsprechend interpretiert werden.

Für die Texte im Kundenprotokoll, die für eine maschinelle Auswertung in Frage kommen, ergibt sich somit folgender Aufbau:

TTTX'20'[NN]

- TTT eigentlicher Text
- X'20 Leerzeichen als Trennung zwischen Text und Nummer
- [NN] 2stellige, in Klammern gesetzte Nummer, die eindeutig sein muss

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Für die maschinelle Auswertung kommen generell die Texte in Frage, die das Ergebnis des DFÜ-Auftrages inklusive Unterschriftsprüfung ausweisen. In der folgenden Tabelle sind die Textnummern und die dazugehörigen Texte, die für eine maschinelle Auswertung in Frage kommen, aufgelistet. Die einzelnen Texte sind in die Bereiche „Datenfernübertragung“, „Elektronische Unterschrift“, „Dateibezogene Nachverarbeitung“ sowie „Bankfachliche Prüfungen“ der Übersichtlichkeit halber unterteilt.

Textnummer	Text
Datenfernübertragung (Bereich 1-20)	
01	Übertragung in Ordnung
02	Abbruch der Übertragung
03	Datenübertragung unverschlüsselt
04	Datenübertragung verschlüsselt
05	Datenübertragung komprimiert
06	Datenübertragung unkomprimiert
07	Keine Daten vorhanden
Elektronische Unterschrift (Bereich 21-50)	
21	Unterschriftsprüfung
22	Zur EU gehörende Originaldatei noch nicht übertragen
23	Unterschrift(en) noch nicht übertragen
24	Unterschrift(en) in Ordnung
25	Unterschrift(en) fehlerhaft
26	Teilnehmer hat mehrfach unterschrieben
27	Keine Unterschriftsberechtigung
28	Unterschrift ist falsch
29	Identische Unterschrift gefunden
30	Falsche Public Key-Version
31	Kein Public Key vorhanden
32	Public Key noch nicht freigegeben
33	Die erforderliche Anzahl von EUs ist nicht vorhanden
34	Angaben zur Originaldatei nicht bei allen EUs identisch
35	Datei nicht prüfbar. Auftrag komplett wiederholen !
36	Aufbau bzw. Grösse der EU-Datei falsch
37	EU-Berechtigung(en) nicht ausreichend
Dateibezogene Nachverarbeitung (Bereich 51-70)	
51	Fehler bei Dekomprimierung
52	Datei nicht lesbar
53	Fehler bei Entschlüsselung
54	Datei ist in ihrem Aufbau fehlerhaft
Bankfachliche Prüfungen (Bereich 71-72)	
71	Keine Berechtigung für Konto
72	Vereinbarter Höchstbetrag überschritten

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Beispiele:

```
14.11.02 11:50:15      Datei zur Bank uebertragen
      Hostname       : HOSTFTAM
      Auftrag        : Beliebige Datei senden                      FTB AAIO
      Teilnehmer     : USER Teilnehmer User
      Ergebnis       : Uebertragung in Ordnung [01]
                     : Datenuebertragung unverschlusselt [03]
                     : Datenuebertragung unkomprimiert [06]
```

```
14.11.02 11:50:15      Datei zur Bank uebertragen
      Hostname       : HOSTFTAM
      Auftrag        : Beliebige Datei senden                      FTB AAJO
      Teilnehmer     : USER Teilnehmer User
      Ergebnis       : Uebertragung in Ordnung [01]
                     : Datenuebertragung verschlusselt [04]
                     : Datenuebertragung komprimiert [05]
```

```
14.11.02 11:51:55      Unterschriftspruefung [21]
      Hostname       : HOSTFTAM
      Auftrag        : Inlandszahlungsverkehrsdatei              IZV AAMO
      Teilnehmer     : USER Teilnehmer User
      Ergebnis       : Unterschrift(en) in Ordnung [24]
      Dateiname      : C:\DAT\IZV1.DTA
```

Displaydatei des Auftrags

```
14.11.02 11:51:55      Unterschriftspruefung [21]
      Hostname       : HOSTFTAM
      Auftrag        : Inlandszahlungsverkehrsdatei              IZV AANO
      Teilnehmer     : USER Teilnehmer User
      Ergebnis       : Unterschrift(en) fehlerhaft [25]
      Dateiname      : C:\DAT\IZV1.DTA
```

Displaydatei des Auftrags

Die erforderliche Anzahl von EUs ist nicht vorhanden [33]

1.7.3 Liste der möglichen Meldungen inklusive Textnummer

Art der Aktion	Meldungs- bzw. Fehlermeldungstexte
Übertragung	Datei zur Bank uebertragen Datei von Bank abgeholt Unterschrift zur Bank uebertragen

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Art der Aktion	Meldungs- bzw. Fehlermeldungstexte
Weiterverarbeitung	Unterschriftspruefung [21] Fehler bei Dekomprimierung [51] Fehler bei Entschluesselung [53] Anzeige Dateiinhalt

Ergebnis der Aktion	Meldungs- bzw. Fehlermeldungstexte
Übertragung	Uebertragung in Ordnung [01] Abbruch der Uebertragung [02] Datenuebertragung unverschlusselt [03] Datenuebertragung verschlusselt [04] Datenuebertragung komprimiert [05] Datenuebertragung unkomprimiert [06]
Weiterverarbeitung	Zur EU gehoerige Originaldatei noch nicht uebertragen [22] Unterschrift(en) noch nicht uebertragen [23] Unterschrift(en) in Ordnung [24] Unterschrift(en) fehlerhaft [25] Fehler bei Dekomprimierung [51] Datei nicht lesbar [52] (<i>nur bei Aktion „Anzeige Dateiinhalt“</i>) Fehler bei Entschluesselung [53] Datei ist in ihrem Aufbau fehlerhaft [54] OK (<i>nur bei Aktion „Anzeige Dateiinhalt“</i>)

Erläuternder Text bei Fehler in der EU-Prüfung	Meldungs- bzw. Fehlermeldungstexte
Auf Teilnehmer bezogene Texte	Teilnehmer hat mehrfach unterschrieben [26] Vereinbarter Hoechstbetrag ueberschritten [72] Keine Unterschriftsberechtigung [27] Teilnehmer hat sich noch nicht initialisiert Teilnehmer noch nicht freigeschaltet Teilnehmer gesperrt Teilnehmereintrag nicht vorhanden Unterschrift ist falsch [28] Identische Unterschrift gefunden [29] Falsche Public Key-Version [30] ²¹ Kein Public Key vorhanden [31] Public Key noch nicht freigegeben [32] Keine Berechtigung fuer Konto [71]

²¹ Diese Meldung wird dann protokolliert, wenn ein Kunde nach dem Umstieg von einer älteren Programmversion (altes EU-Format) auf eine neue Programmversion (neues EU-Format) Unterschriftsdateien an das Kreditinstitut schickt, ohne sich vorher neu initialisiert beziehungsweise eine Public Key-Änderung durchgeführt zu haben.

DFÜ – Abkommen

Anlage 1 (Standards für die Kommunikation)

Erläuternder Text bei Fehler in der EU-Prüfung	Meldungs- bzw. Fehlermeldungstexte
Allgemeine Texte	Die erforderliche Anzahl von EUs ist nicht vorhanden [33] Angaben zur Originaldatei nicht bei allen EUs identisch [34] Datei nicht prüfbar. Auftrag komplett wiederholen ! [35] <i>(Diese Meldung wird ausgegeben, wenn eine Betriebsstörung bei der Unterschriftsprüfung auftritt, z.B. zu wenig Speicherplatz)</i> Aufbau bzw. Grösse der EU-Datei falsch [36] EU-Berechtigung(en) nicht ausreichend [37]

1.7.4 Dateianzeige auf Kunden- und Bankseite

Auftragsarten für Dateien im DTAUS-Format:

	Aus Feldnummer der DTAUS-Spezifikation
Überschrift	
Zahlungsart	A3
Bankleitzahl	A4
Kontonummer	A9
Auftraggeber	A6
Erstellungsdatum	A7
Anzahl der Zahlungssätze	E4
Summe der Beträge (EUR)	E8
Summe der Kontonummern	E6
Summe der Bankleitzahlen	E7
Ausführungstermin	A11b

Beispiel:

G U T S C H R I F T E N

Bankleitzahl	: 30040000
Kontonummer	: 0825112600
Auftraggeber	: BANK-VERLAG
Erstellungsdatum	: 10.05.00
Anzahl der Zahlungssätze	: 1
Summe der Beträge (EUR)	: 10.000,00
Summe der Kontonummern	: 00000000001234567
Summe der Bankleitzahlen	: 00000000007654321
Ausführungstermin	: 10.05.2000

Abbildung 1.9 Auftragsarten für Dateien im DTAUS-Format

Auftragsarten für Dateien im DTAZV-Format:

	Aus Feldnummer der DTAUS-Spezifikation
Überschrift	
Bankleitzahl	Q3
Kundennummer	Q4
Auftraggeberdaten	Q5
Erstellungsdatum	Q6
T-Satz-Informationen	
Auftragswährung	T13
Bankleitzahl	T3
Kontowährung	T4a
Kontonummer	T4b
Ausführungstermin	T5
Betrag	Summe der Felder T14a und T14b aller T-Sätze, bei denen die voranstehenden Felder T13, T3, T4a, T4b und T5 identisch belegt sind. Bei abweichender Belegung in derselben Datei werden diese T-Satz-Informationen entsprechend mehrfach angegeben.
Anzahl der Datensätze T	Kontrollsumme aus Feld Z4
Summe der Beträge	Kontrollsumme aus Feld Z3

Beispiel:

Bankleitzahl	: 30040000
Kundennummer	: 0000000001
Auftraggeberdaten	: KARL MUSTERMANN MUSTERSTR. 1 50825 KOELN
Erstellungsdatum	: 10.05.00
Auftragswährung	: ILS
Bankleitzahl	: 30040000
Kontowährung	: EUR
Kontonummer	: 1234567890
Ausführungstermin	: 10.05.00
Betrag	: 20.000,000
Anzahl der Datensätze T	: 000000000000001
Summe der Beträge	: 000000002000000

Abbildung 1.10 Auftragsarten für Dateien im DTAZV-Format

2 Anlage 2 (Standards für die Sicherheit)

2.1 Festlegungen / Symmetrischer Algorithmus

Als Basisverschlüsselungsroutine wird der 2-Key-Triple-DES im CBC Modus gemäß ISO 10116 (ANSI X3.106) verwendet (vgl. Abbildung 2.1).

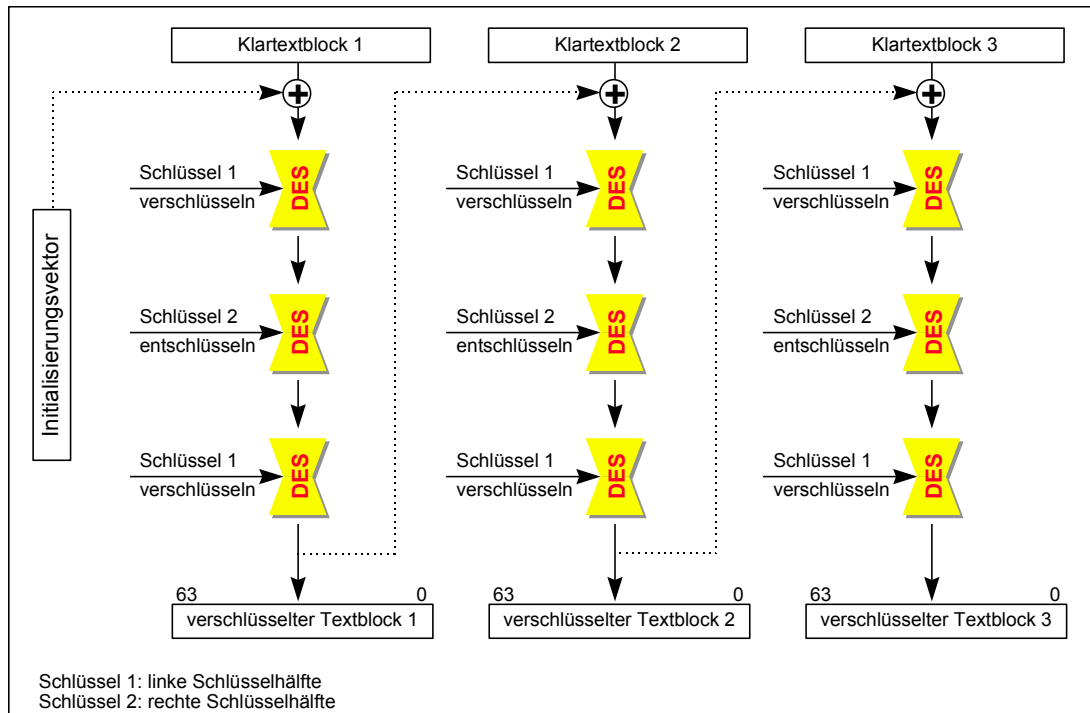


Abbildung 2.1: 2-Key-Triple-DES im CBC-Mode

Der Initial Chaining Value (ICV) wird auf X'00 00 00 00 00 00 00 00' festgelegt.

Die generierten Zufallszahlen, die als rechte und linke Schlüsselhälfte des 2-Key-Triple-DES verwendet werden, sind daraufhin zu überprüfen, dass es sich nicht um einen der in der nachfolgenden Tabelle aufgelisteten schwachen oder halbschwachen DES-Schlüssel handelt.

Die schwachen Schlüssel des DES							
01	01	01	01	01	01	01	01
FE	FE	FE	FE	FE	FE	FE	FE
1F	1F	1F	1F	0E	0E	0E	0E
E0	E0	E0	E0	F1	F1	F1	F1
Die halbschwachen Schlüssel des DES							
01	FE	01	FE	01	FE	01	FE
FE	01	FE	01	FE	01	FE	01
1F	E0	1F	E0	0E	F1	0E	F1
E0	1F	E0	1F	F1	0E	F1	0E
01	E0	01	E0	01	F1	01	F1
E0	01	E0	01	F1	01	F1	01
1F	FE	1F	FE	0E	FE	0E	FE
FE	1F	FE	1F	FE	0E	FE	0E
01	1F	01	1F	01	0E	01	0E
1F	01	1F	01	0E	01	0E	01
E0	FE	E0	FE	F1	FE	F1	FE
FE	E0	FE	E0	FE	F1	FE	F1

2.2 Kryptographische Verfahren des deutschen Kreditgewerbes für die Elektronische Unterschrift im Rahmen der Kunde-Bank-Kommunikation

2.2.1 Allgemeine Anforderungen

Die zum Einsatz kommenden Sicherheitsverfahren müssen die Elektronische Unterschrift für die zu übertragenden Daten leisten. Hierbei ist folgendes Anforderungsprofil zu erfüllen:

- Die Unterschrift darf nur vom Unterzeichner geleistet werden können, so dass der Unterzeichner die Unterschrift nicht leugnen kann bzw. dass beweisbar ist, dass der Ursprung eines eventuellen Missbrauchs nur im Verantwortungsbereich des Unterzeichners liegen kann.
- Jeder mögliche Empfänger muss die Echtheit der Unterschrift prüfen können, wobei zusätzlich gewährleistet sein muss, dass diese Prüfung auch zu einem späteren Zeitpunkt (z. B. durch juristische Instanzen) möglich ist.
- Die Unterschrift muss in einem direkten Zusammenhang zu dem unterschriebenen Dateiinhalt stehen, so dass sie gleichzeitig den entsprechenden Dateiinhalt authentifiziert und so jeder mögliche Empfänger (insbesondere juristische Instanzen auch noch zu einem späteren Zeitpunkt) anhand der Unterschrift auch den Dateiinhalt verifizieren kann (Prüfung der Dateiintegrität).
- Die Unterschriftslösung muss auf jeden beliebigen Kontext anwendbar sein.
- Das Unterschriftenverfahren muss unter Performancegesichtspunkten auch auf weniger leistungsfähigen PC mit vertretbarer Rechenzeitintensität einsetzbar sein.
- Der Verwaltungsaufwand für die notwendige Aufbewahrung der zur Unterschriften-erzeugung und insbesondere -prüfung benötigten Daten (Kennungen) muss möglichst gering sein (einfaches Key Management).
- Die konkrete technische Lösung muss für die gängigen Betriebssysteme, die beim Unterzeichner bzw. Empfänger zum Einsatz kommen können, kompatibel einsetzbar sein.

Dieses Anforderungsprofil kann nur durch den Einsatz asymmetrischer kryptographischer Verfahren erfüllt werden.

Die Verwendung der Elektronischen Unterschrift ist für alle Datenübertragungen zwingend vorgeschrieben, die nicht der reinen Informationsbeschaffung dienen, soweit in den besonderen Vereinbarungen für einzelne Verfahren nichts Abweichendes bestimmt ist.

Für jedes konkret zum Einsatz kommende Sicherheitsverfahren muss eine detaillierte Beschreibung der darin verwendeten mathematischen Verfahren sowie der verwendeten Datenstrukturen kostenlos offengelegt werden. Diese Beschreibung muss geeignet sein, ein funktional kompatibles Produkt durch beliebige Hersteller erstellen zu lassen. Außerdem muss ein positives Gutachten eines vom Kreditgewerbe bestimmten Gutachters zu dem jeweiligen Gesamtverfahren und speziell zu den darin zum Einsatz kommenden mathematischen Prozeduren vorgelegt werden.

2.2.2 Elektronische Unterschrift der Version A003

Für die Kreditinstitute besteht bis zum 31. Dezember 2004 die Verpflichtung zur Unterstützung der Version A003.

Unter Beachtung der oben genannten Festlegungen ist derzeit das nachfolgend beschriebene Verfahren für die Elektronische Unterschrift zugelassen.

2.2.2.1 Festlegungen

Asymmetrischer Algorithmus:

Derzeit wird das RSA-Verfahren eingesetzt. Dabei werden folgende Eigenschaften vorausgesetzt:

- Es wird ein konstanter öffentlicher Exponent e und ein für jeden Kunden individueller Modulus n für jedes eingesetzte RSA-Schlüsselsystem verwendet.
- 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:

$$2^{N-1} \leq n < 2^N$$

- Der Zielwert für N ist 768, wobei eine aus der Suche nach starken Primzahlen resultierende Unterschreitung dieses Wertes um maximal 60 Bit zulässig ist.

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 Primteiler r .
 $p + 1$ hat einen großen Primteiler s .
 $r - 1$ hat einen großen Primteiler.

- Die gleichen Forderungen werden an q gestellt.
- Die Längen von p und q sollen sich um höchstens 12 Bits unterscheiden.
- Der konstante öffentliche Exponent e wird für die Elektronische Unterschrift auf die 4. Fermatsche Primzahl festgelegt: $e = 2^{16} + 1$
- Bei der Wahl von p und q ist sicherzustellen, dass e kein Primfaktor von $p - 1$ oder $q - 1$ ist.

Hash-Algorithmus:

Derzeit wird der mit DFP bezeichnete Hash-Algorithmus benutzt. Basis für die Erzeugung dieses Hashwertes ist der Data Encryption Standard (DES, ANSI X3.92). M sei definiert als ein Datenblock beliebiger Länge. M wird durch Hinzufügen von Nullen auf der rechten Seite aufgefüllt, bis ein Vielfaches von 8 Bytes vorliegt (Paddingregel). Die 8 Bytes-Blöcke, deren Verkettung M ergibt, seien mit M_i ($1 \leq i \leq m$) bezeichnet. Die Funktion $DES(b,k)$ bezeichnet die DES-Verschlüsselung eines 8 Byteslangen Blockes b mit dem Schlüssel k . Mit \otimes wird nachfolgend eine Exklusiv-Oder-Funktion (XOR) bezeichnet.
 o_i sind Blöcke der Länge 8 Bytes mit

$$o_{-1} = 0;$$
$$o_0 = 0.$$

o_i berechnet sich für $i = 1$ bis m iterativ wie folgt:

$$o_i = M_i \otimes \text{DES}((M_i \otimes o_{i-1} \otimes o_{i-2} \otimes x), k)$$

Dabei ist (in hexadezimaler Darstellung)

$$x = X \text{ '01 23 45 67 89 AB CD EF'}$$

Die beiden letzten entstehenden Blöcke o_{m-1} und o_m seien mit $f_1(M,k)$ und $f_2(M,k)$ bezeichnet. Unter Verwendung von 2 verschiedenen Schlüsseln k_1 und k_2 werden zunächst berechnet:

- $c_1 = f_1(M, k_1)$
- $c_2 = f_2(M, k_1)$
- $c_3 = f_1(M, k_2)$
- $c_4 = f_2(M, k_2)$

Dabei sind (in hexadezimaler Darstellung)

- k_1 : X '902628CBEC461543'
- k_1 mit gerader Parität: X '902728CAED471442'
- k_1 mit ungerader Parität: X '912629CBEC461543'
- k_2 : X '2A41522F4446502A'
- k_2 mit gerader Parität: X '2B41532E4447502B'
- k_2 mit ungerader Parität: X '2A40522F4546512A'

Es wird eine Funktion G definiert, deren Ergebnis in Abhängigkeit von den jeweils 8 Bytes langen Variablen x , y und k ebenfalls 8 Bytes umfaßt. Dabei gilt:

$$G(x,y,k) = \text{DES}((x \otimes y), k) \otimes \text{DES}(x,k) \otimes \text{DES}(y,k) \otimes y$$

So werden gebildet:

$$\text{FP1} = G(G(c_1, c_2, k_1), G(c_3, c_4, k_1), k_1) \text{ und}$$
$$\text{FP2} = G(G(c_1, c_2, k_2), G(c_3, c_4, k_2), k_2).$$

Der 16 Bytes lange, hier mit DFP bezeichnete Hashwert HASH ist dann die Verkettung dieser beiden Werte:

$$\text{DFP} = (\text{FP1}, \text{FP2})$$

2.2.2.2 Definitionen

Verwendete Symbole	Bedeutung / Wert
N	Modulus eines RSA-Schlüsselsystems
N	Länge von N in Anzahl der Bit
HASH	Hashwert
THASH	Time stamped HASH
SIGNATUR	Signatur der nachricht
TVP	Zeitstempel (Time Variant Parameter)

2.2.2.3 Voraussetzungen

Für die Anwendung dieser Spezifikationen ist folgendes zu beachten:

- Für die Erzeugung der Elektronischen Unterschrift gilt die Paddingregel des jeweiligen Hash-Algorithmus (gemäß dem oben beschriebenen Hash-Algorithmus).
- Für die Erzeugung und Verifikation der Elektronischen Unterschrift verwendeten asymmetrischen Algorithmen sind oben unter „Asymmetrischer Algorithmus“ näher spezifiziert.
- Die im Folgenden verwandten Längenangaben setzen im Falle der Elektronischen Unterschrift stets eine Hashwertlänge von 128 Bit voraus (siehe oben unter „Hash-Algorithmus“). Sollte zukünftig ein Hash-Algorithmus mit einer anderen Hashwertlänge Verwendung finden, so sind die Längenangaben entsprechend anzupassen.
- Der aus dem zu unterschreibenden Text resultierende Hashwert wird vor der Erzeugung der Elektronischen Unterschrift um den aktuellen Zeitstempel ergänzt. Dieses bewirkt, dass zwei Aufträge, die inhaltlich identisch sind, anhand der Zeitangabe unterschieden werden können. Damit ist der Empfänger in der Lage, zwei identische Aufträge vor der doppelten Einreichung eines Auftrages zu unterscheiden. Eine Manipulation der Zeitwerte während der Datenübertragung durch Außentäter kann durch die Einbeziehung der Werte in die Elektronische Unterschrift erkannt werden.
- Es wird generell ASCII als Zeichensatz verwendet.

2.2.2.4 Sicherung der Nachrichten**Vorgänge beim Sender: Erzeugung der elektronischen Unterschrift:**

Es wird ein Hashwert über die Originalnachricht berechnet. Dieser Hashwert wird formatiert und das Ergebnis wird signiert.

Hashwertberechnung:

Padding der Nachricht: Das Padding der Nachricht erfolgt nur temporär, um den Hashwert

berechnen zu können. Die genaue Festlegung der Paddingregel wird in Abhängigkeit von den verwendeten Hash-Algorithmen (siehe oben „Hash-Algorithmus“) definiert.

Anwendung des Hashalgorithmus: Die Hashwertberechnung erfolgt abhängig von dem verwendeten Hash-Algorithmus. Die Einzelheiten sind oben unter „Hash-Algorithmus“ zu sehen.

Der Hashwert hat eine Länge von 128 Bit und wird HASH genannt.

$\text{HASH} = Y_{128}, Y_{127}, \dots, Y_1$

Signatur des Hashwertes:

Der aus dem zu unterschreibenden Text resultierende Hashwert wird vor der Erzeugung der Elektronischen Unterschrift um den aktuellen Zeitstempel (TVP) ergänzt, der den Zeitpunkt der geleisteten Unterschrift dokumentiert. Anhand des Zeitstempels können zwei inhaltlich identische Aufträge unterschieden werden. Damit ist der Empfänger in der Lage, zwei identische Aufträge von der doppelten Einreichung eines Auftrages zu unterscheiden. Eine Manipulation der Zeitwerte während der Datenfernübertragung durch Außentäter kann durch die Einbeziehung der Werte in die Elektronische Unterschrift erkannt werden.

Der Wert der Elektronischen Unterschrift hängt daher nicht ausschließlich vom Hashwert der Nachricht ab, sondern auch von den angehängten Bits des Zeitstempels TVP.

Es wird eine Binärfolge THASH mit einer Länge von 256 Bit gebildet, die aus dem aktuellen Zeitstempel der Elektronischen Unterschrift und HASH besteht. Die niedrigwertigen 128 Bit von THASH enthalten den Zeitstempel TVP.

Der Zeitstempel hat das Format: **jjjjmmttX'20'hhppssX'20'**

Symbol	Bedeutung	Anzahl Bytes
jjjj	Jahr	4
mm	Monat	2
tt	Tag	2
X'20'	<i>Leerzeichen</i>	1
hh	Stunde	2
pp	Minute	2
ss	Sekunde	2
X'20'	<i>Leerzeichen</i>	1

Die Gesamtlänge von TVP beträgt 16 Bytes (128 Bit).

Es sei $\text{THASH} = (z_{256}, z_{255}, \dots, z_1)$ mit $\text{TVP} = (z_{128}, \dots, z_1)$ und $\text{HASH} = (z_{256}, \dots, z_{129})$.

Der geheime Schlüssel des RSA-Schlüsselsystems des Erzeugers der Elektronischen Unterschrift wird verwendet, um die Binärfolge THASH digital zu unterschreiben. Das Ergebnis heißt SIGNATUR.

Übermittlung:

An den Kommunikationspartner wird die Originalnachricht (ohne die Bits, die als Padding für die Hashwertberechnung angefügt wurden) und ggf. die Elektronische Unterschrift des Senders (SIGNATUR) übertragen. Die genauen Formate sind dem Kapitel 2.2.2.5 Formate zu entnehmen.

Vorgänge beim Empfänger: Verifikation der Elektronischen Unterschrift:

Erhalt des übermittelten Hashwertes:

Unter Verwendung des öffentlichen Schlüssels des Absenders wird aus der Bitfolge SIGNATUR die Bitfolge THASH in der Länge von 256 Bit ermittelt.

Die niedrigstwertigen 128 Bit von THASH werden als Zeitstempel interpretiert. Die Darstellung des Zeitstempels ist in Kapitel 0 definiert.

Die 128 höchstwertigen Bit von THASH bilden den Hashwert HASH, die der Empfänger als Begleitinformation für die Nachricht erhalten hat.

Berechnung des Hashwertes:

Die Berechnung des Hashwertes über die empfangene Nachricht erfolgt wie oben unter Hashwertberechnung beschrieben.

Dieser Hashwert heißt HASH'.

Vergleich der Hashwerte:

Abschließend wird verglichen, ob der empfangene Hashwert HASH und der selbst berechnete Hashwert HASH' identisch sind.

Ist dies der Fall, so ist die empfangene Nachricht unversehrt und authentisch.

2.2.2.5 Formate

Für die Sicherheitservices auf dem Nachrichtenlevel werden die folgenden Grundanforderungen definiert:

- Authentikation
- Integrität
- Non-Repudiation

Authentikation, Integrität und Non-Repudiation werden mittels der Elektronischen Unterschrift verwirklicht. Die Elektronische Unterschrift bzw. bei Mehrfachunterschriften die Elektronischen Unterschriften werden in einer separaten „EU-Datei“ abgelegt.

Diese Datei enthält je Elektronischer Unterschrift folgenden 512 Bytes langen Datensatz:

DFÜ – Abkommen

Anlage 2 (Standards für die Sicherheit)

Inhalt	Länge in Bytes ²²	Erläuterung/Belegung
Versionsnummer	an 4	‚A003‘
Länge des Modulos	n 4	‚0768‘
Auftragsart	an 3	Auftragsartkürzel der Originaldatei gemäß den Standards für die Kommunikation Kapitel 1.4 Auftragsartenkennungen) z. B. ‚IZV‘
EU	binär 128	rechtsbündig, ‚0, ..., 0, SIGNATUR‘
UserID	an 8	z. B. ‚A2B2C2D2‘
Originaldatei	an 128	lokaler Dateiname der Originaldatei
Datum/Uhrzeit der Dateierstellung	an 16	jjjjmmTtX‘20‘hhppssX‘20‘ (siehe Signatur des Hashwertes in Kapitel 2.2.2.4 „Sicherung der Nachrichten“.
Datum/Uhrzeit der Unterschrift	an 16	jjjjmmTtX‘20‘hhppssX‘20‘ (siehe Signatur des Hashwertes in Kapitel 2.2.2.4 „Sicherung der Nachrichten“.
frei nutzbares Feld	binär 8	zur Zeit nicht genutzt; X‘00‘
Reserve	binär 197	zur Zeit nicht genutzt; X‘00‘

2.2.2.6 Beschreibung der Abläufe

Für das Verfahren der Elektronischen Unterschrift werden fünf Funktionen genutzt:

1. Keypaar-Generierung kundenseitig
2. Berechnung eines Fingerprints (Verhashung) bank- und kundenseitig
3. Signieren einer Datei (Erstellung einer EU) kundenseitig
4. Verifizieren der Signatur (Prüfung der EU) bankseitig
5. Änderung des Paßwortes für den Secret Key kundenseitig

Daten zur Identifikation und Legitimation des Kunden:

User-ID: Max. 8stellig alphanummerisch (wird vom jeweiligen Kreditinstitut frei vergeben)

Host-ID: Max. 8stellig alphanummerisch (wird vom jeweiligen Kreditinstitut vergeben)

Original-Passwort: Max. 8stellig alphanummerisch (erlaubt dem User den Zugang zu den verschiedenen Bankrechnern)

Password: Für jedes Kreditinstitut gelten unterschiedliche, aus dem Original-Passwort nach Voranstellen der max. achtstelligen Host-ID unter Verwendung der nachfolgend beschriebe-

²² an = alphanummerisch; n = numerisch. Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X‘20‘) aufgefüllt. Werte im Binär-Format werden rechtsbündig eingestellt und links mit X‘00‘ aufgefüllt.

nen Hashfunktion abgeleitete Passworte (Hashwerte), die nicht auseinander berechenbar sind (Multi-Bankfähigkeit)

Verhasht werden nur die tatsächlich belegten Zeichen von Bankkennung und Passwort. Als Hash-Funktion wird das im Folgenden beschriebene Verfahren verwendet:

- Ein zu bearbeitender Datenstring x (ASCII-Darstellung) der Länge $2n$ wird in die Blöcke x_1, x_2, \dots, x_n von je 2 Bytes Länge unterteilt. Hat der Datenstring x eine ungerade Länge, so wird er mit einem Byte $X'FF'$ aufgefüllt (*Padding*).
- Jeder aus 4 Halbbytes bestehende Block x_i wird nun zu einem Block y_i doppelter Länge transformiert, indem jedem Halbbyte 4 binäre Einsen ($X'F'$) vorangestellt werden (*Zo-ning*).

Beispiel: $x_i = X'A18E' \rightarrow y_i = X'FAF1F8FE'$

- In einem iterativen Prozeß werden nun die einzelnen Blöcke verknüpft, indem Elemente h_i nach folgender Vorschrift gebildet werden (*Quadratur modulo m*):

$$h_1 = y_1^2 \bmod m$$

$$h_i = (h_{i-1} \otimes y_i)^2 \bmod m \quad (i = 2, \dots, n)$$

Als Modulo wird die Primzahl $X'B61A2CA7'$ (3.055.168.679) verwendet. Die Verknüpfung \otimes ist die bitweise Addition modulo 2 (XOR-Operation). Der Hashwert $H(x)$ des Datenstrings x wird definiert als $H(x) = h_n$

- Dieser binäre Wert von 32 Bit Länge wird nun in eine aufbereitete lesbare Darstellung $H'(x)$ gebracht, indem das übliche Dump-Format gebildet wird, so dass als Ergebnis ein Datenstring von 8 Bytes Länge und dem Wertebereich 0, ..., 9, A, ..., F entsteht (*Presentation*).

Beispiel: $H(x) = X'259AEEB1' \rightarrow H'(x) = \text{„259AEEB1“ (ASCII)}$
 $= X'3235394145454231'$

Die beim Kreditinstitut über das Passwort zugänglichen Funktionen werden von den Kreditinstitut einzeln und User-spezifisch festgelegt. Das Kreditinstitut vergibt an einen neuen Benutzer zunächst ein Initial-Passwort mit dem Wert „start“, das beim Kreditinstitut als entsprechender Hashwert „H“ (Bankkennung und Passwort) gespeichert wird. Mit diesem Passwort ist nur die Berechtigung zu einer Passwort- und Public-Key-Änderung verbunden, die der User als erstes durchzuführen hat (Initialisierung). Bei der Initialisierung (Auftragsart „INI“) wird

- das geänderte Passwort (Hashwert) dem Bankrechner mitgeteilt,
- eine Datei übertragen, die bei Verfügbarkeit der EU den Public-Key des Users enthält und sonst aus einem Blank besteht,
- am PC ein Ausdruck (INI-Brief) mit folgenden Daten veranlaßt:
Benutzername / Datum / Uhrzeit / Empfänger-Bank / User-ID (externe) / Kunden-ID / EU-Versionsnummer / definierte Längenangabe des Public-Key / Public-Key / Längenangabe des Modulus / Modulus / DFP-Hashwert über den Public-Key (Exponent und Modulo) in 4 Zeilen à 8 Zeichen (4 Bytes). (Beispiel für den Ausdruck des INI-Briefes am Ende dieses Kapitels 2.2.2.6). Das ausgedruckte Formular (INI-Brief) sendet der Benutzer unterschrieben an die Bank, die daraufhin erst die vereinbarten Transaktionen des Users freigibt. Bei vergessenen Passwörtern setzt sich der Kunde mit der zuständigen Bank in Verbindung, um erneut ein Initial-Passwort mit dem Wert „start“ zu erhalten.

Beispiel:

Im folgenden werden die Anwendungen dieser Funktionen anhand eines Beispiels beschrieben. Parameter für dieses Beispiel:

Parameter	Wert
Kunden-ID	'A1B1C1D1'
User-ID	'A2B2C2D2'
Exponent	0...010001 (Hex)
Lmodulo	'0768'
Modulo	0...bc7bdc...87 (Hex)
Auftragsart Originaldatei	'TST'
Auftragsart Unterschrift	'TST'
Auftragsnummern	'A000'
FTAM spezifische Parameter:	
Host-ID	'A3B3C3D3' (8-stellig, alphanummerisch)
Password	8-stellig, alphanummerisch

Key-Paar-Generierung und Verteilung des Public-Key

Kundenseite Rahmenprogramm:

- Erzeugung und Speicherung von Public-Key und Private Key
- Generierung der Public-Key-Datei:
(Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks X'20' aufgefüllt. Werte im Binär-Format werden rechtsbündig eingestellt und links mit X'00' aufgefüllt)

Inhalt	Anzahl Bytes	Belegung / Erläuterung
Versionsnummer	4 ASCII	'A003' Dieses Feld dient zur Kennzeichnung des verwendeten EU-Verfahrens (A003).
User-ID	8 ASCII	'A2B2C2D2' Dieses Feld enthält die institutsabhängige User-ID. Dies hat zur Folge, dass das Kundensystem vor dem Versenden der Public Key-Datei die entsprechende User-ID eintragen muss.
LExponent	4 ASCII	'0768', Länge des Exponenten, Wert in Bit
Exponent	128 binär	00...010001 (Hex) Dieses Feld kann Werte bis maximal 1024 Bit enthalten.
LModulo	4 ASCII	'0768', Länge von Modulo, Wert in Bit
Modulo	128 binär	0...bc7bdc...87 Dieses Feld kann Werte bis maximal 1024 Bit enthalten.
Reserve	236 ASCII	Auffüllen mit X'20'

DFÜ – Abkommen

Anlage 2 (Standards für die Sicherheit)

- Anlegen eines DFÜ-Auftrages des Typs INI (Initialisierung)
A3.A1B1C1D1.INI.DNNNN.A000
FTAM-spezifische Felder
- Übertragung der Public-Key-Datei
- Versand des INI-Briefes an die Bank

Bankseite Rahmenprogramm:

- Lesen Public-Key-Datei
- Eingabe des Hashwertes aus INI-Brief des Kunden (optional)
- Prüfung von Public-Key und Hashwert über Kryptographie-Funktion (optional)
- Protokollierung des Public-Keys, des Hashwertes sowie des Prüfungsergebnisses (optional) Beispiel: PUB.PTK
- Im Erfolgsfall: Freischaltung des Teilnehmers, Speicherung des Keys
Neuer Status des Teilnehmers: ‚BEREIT‘
- Im Fehlerfall: Eingabewiederholung oder Löschung der Public-Key-Datei
- Protokollierung des Initialisierungsvorganges im Kundenprotokoll A1B1C1D1.PTK

Ablauf der Elektronischen Unterschrift

Kundenseite Rahmenprogramm:

- Bildung eines Fingerprints durch Verhashung der Originaldatei. Betriebssystem-abhängige Zeichen (*bei DOS CR, LF, CRLF und Control-Z*) gehen in die Bildung des Hashwertes nicht mit ein.
- Einfügen des Zeitstempels
- Bildung der Signatur des Hashwertes
- Erstellung der EU-Datei
- Generierung zweier DFÜ-Aufträge:
A3.A1B1C1D1.TST.ONNNN.A000 (für die Originaldatei)
A3.A1B1C1D1.TST.UNNNN.A000 (für die Unterschriftsdatei)
- Übertragung der Dateien innerhalb des bankseitig festgelegten Zeitfensters

Bankseite Rahmenprogramm:

- Falls O-Datei und zugehörige U-Datei vorhanden, erfolgt Prüfung (O-Datei:
O\TST\A1B1C1D1.A000, ggf. U-Datei: U\TST\A1B1C1D1.A000)

Auf Bankseite wird ein zeitlicher Rahmen definiert, innerhalb dessen zusammengehörige Original- und Unterschriftsdateien eingetroffen sein müssen.

- Bildung des Fingerprints über die O-Datei durch Verhashung
- Erweitern des Fingerprints durch Datum/Uhrzeit der EU aus EU-Datei
- Verifizierung
- EU-Protokoll
(Informationen aus EU-Datei, Public Key, A-/E-Satz der O-Datei, Prüfungsergebnisse)
Beispiel: EU.PTK
- Erfolgsfall bei EU-Prüfung: Weiterleitung der O-Datei
- Fehlerfall bei EU-Prüfung : Ablehnung der O-Datei
- Archivierung nach den einschlägigen handels- und steuerrechtlichen Vorschriften unter Berücksichtigung der Grundsätze ordnungsgemäßer Speicherbuchführung
- Eintrag ins Kundenprotokoll (A1B1C1D1.PTK)

Abholen der Kundenprotokolle

- Einrichten eines DFÜ-Auftrags PTK zum Abholen des Kundenprotokolls
'A3.A1B1C1D1.PTK.DNNNN'/FTAM-spezifische Felder
Dort verzeichnet sind z. B.:
Annahme bzw. Ablehnung des Public Keys, Ergebnis jeder EU-Prüfung, Annahme einer Kundendatei, Ergebnisse aus der Weiterverarbeitung, usw.
- Übertragung des Kundenprotokolls
Beispiel: A1B1C1D1.PTK

DFÜ – Abkommen

Anlage 2 (Standards für die Sicherheit)

Beispiel für einen INI-Brief DFÜ (A003):

Benutzername	system	Kundensoftware-interner Name (Angabe freigestellt)
Datum	TT.MM.JJJJ	Datum der Erstellung des Initialisierungs- bzw. Public-Key-Änderungsauftrages
Uhrzeit	HH:MM	Uhrzeit der Erstellung des Initialisierungs- bzw. Public-Key-Änderungsauftrages
Empfänger	DFÜ-Bank	Hostname der Bank (max. 8 Stellen; wird von der jeweiligen Bank mitgeteilt)
User-ID	xxxxxxx	(8 Bytes alphanummerisch; beginnend mit einem Alphazeichen; wird von der jeweiligen Bank mitgeteilt)
Kunden-ID	yyyyyyy	(8 Bytes alphanummerisch; wird von der jeweiligen Bank mitgeteilt)
EU-Version	A003	

Öffentlicher Schlüssel (Public-Key) für die Elektronische Unterschrift:

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

Modulo	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	D7	4A	2F	D5	6C	16	4E	C3	2D	82	F3	02	31
CD	FF	FB	45	77	E4	7E	E5	B2	CB	7B	9A	5F	75	7B	32
7C	16	E5	FB	16	41	0B	4A	39	OF	50	47	68	9C	9B	27
D2	A0	9C	CA	23	A8	C3	1C	AB	A5	ED	72	75	9D	0A	B8
9B	37	BA	00	CB	68	BB	AC	C8	D1	C8	D3	35	C8	BF	1F
A3	06	CF	24	5A	DC	EB	84	64	86	D0	97	8f	E4	67	08

Hash	5D F9 15 F4
	3D 78 69 D5
	00 80 60 E5
	9A 4C 87 5A

Ich bestätige hiermit den obigen öffentlichen Schlüssel für meine Elektronische Unterschrift.

Ort / Datum

Firma / Name

Unterschrift

2.2.2.7 Testdaten Elektronische Unterschrift²³**Elektronische Unterschrift: Beispiel 1**

Testdatei: 00548495.DTA - 3072 Bytes

Hashfunktion: AR/DFP

k1:	90	26	28	CB	EC	46	15	43
k2:	2A	41	52	2F	44	46	50	2A

768-Bit RSA Schlüssel 1

Modulus:

BC	7B	DC	71	12	56	E8	BD	-	B4	A0	CA	EB	B5	DB	B2	ED
CD	5F	78	70	29	A8	E6	AD	-	84	84	A1	D1	E8	C9	E1	2D
A0	2F	4B	70	AC	06	84	7C	-	35	D1	0E	79	4E	C6	E9	0D
43	70	62	AE	66	4B	A1	C8	-	05	00	F1	AD	7C	69	C6	23
0C	47	6E	C5	86	3B	40	F8	-	4A	76	06	AD	79	32	1C	4F
10	9F	87	C6	52	45	03	3F	-	2A	8B	A0	6E	21	91	13	87

Öffentlicher Exponent:

01 00 01

Geheimer Exponent:

08	A2	7A	A8	7F	6E	40	7E	-	A3	03	69	68	6A	4E	0F	4B
64	F3	86	61	4A	61	F4	CC	-	BC	31	15	7F	62	27	BA	CB
76	A1	7E	B3	97	08	91	67	-	33	51	49	78	20	8B	63	07
36	E0	CC	52	0F	D2	08	27	-	7B	6B	C5	FD	A1	39	41	1C
90	D9	93	B8	C5	18	48	06	-	FA	2C	49	EC	42	09	1C	F8
5E	86	C1	8A	47	0A	ED	3F	-	81	1E	57	95	A1	5E	5D	71

Hashwert:

AA	05	85	78	F9	A2	F7	EE	-	FF	E7	F4	B0	35	19	83	0F
----	----	----	----	----	----	----	----	---	----	----	----	----	----	----	----	----

Elektronische Unterschrift:

6C	43	52	5A	20	F8	2F	00	-	CA	B2	A4	71	AB	62	12	7B
85	DD	9E	0A	7E	8C	45	82	-	B6	A8	D9	E7	4F	E8	E4	E6
3C	46	93	71	1F	5A	42	9C	-	B0	3F	B2	0A	C1	81	13	72
D7	82	B2	9A	8A	F3	12	66	-	79	3A	4C	EC	81	CE	A1	30
7A	8D	D3	2E	B0	DB	30	43	-	BB	F7	50	F4	4D	BD	43	A9
0C	A5	D0	18	48	F0	9B	88	-	2E	77	9E	C7	D6	BF	5B	F4

²³ Die Testdateien 00548495.DTA und 00548495.ZKA sind beim jeweils federführenden ZKA-Verband hinterlegt und können dort bezogen werden.

Elektronische Unterschrift: Beispiel 2

Testdatei: 00548495.ZKA - 1376 Bytes

Hashfunktion: AR/DFP

k1:	90	26	28	CB	EC	46	15	43
k2:	2A	41	52	2F	44	46	50	2A

768-Bit RSA Schlüssel 1

Modulus:

BC	7B	DC	71	12	56	E8	BD	-	B4	A0	CA	EB	B5	DB	B2	ED
CD	5F	78	70	29	A8	E6	AD	-	84	84	A1	D1	E8	C9	E1	2D
A0	2F	4B	70	AC	06	84	7C	-	35	D1	0E	79	4E	C6	E9	0D
43	70	62	AE	66	4B	A1	C8	-	05	00	F1	AD	7C	69	C6	23
0C	47	6E	C5	86	3B	40	F8	-	4A	76	06	AD	79	32	1C	4F
10	9F	87	C6	52	45	03	3F	-	2A	8B	A0	6E	21	91	13	87

Öffentlicher Exponent:

01 00 01

Geheimer Exponent:

08	A2	7A	A8	7F	6E	40	7E	-	A3	03	69	68	6A	4E	0F	4B
64	F3	86	61	4A	61	F4	CC	-	BC	31	15	7F	62	27	BA	CB
76	A1	7E	B3	97	08	91	67	-	33	51	49	78	20	8B	63	07
36	E0	CC	52	0F	D2	08	27	-	7B	6B	C5	FD	A1	39	41	1C
90	D9	93	B8	C5	18	48	06	-	FA	2C	49	EC	42	09	1C	F8
5E	86	C1	8A	47	0A	ED	3F	-	81	1E	57	95	A1	5E	5D	71

Hashwert:

0F	8E	CD	36	27	D8	49	16	-	C4	2C	65	D5	7A	9B	97	8A
----	----	----	----	----	----	----	----	---	----	----	----	----	----	----	----	----

Elektronische Unterschrift:

5B	A8	CE	C1	EF	06	A0	DC	-	38	D3	B6	2B	5A	AA	05	F8
BB	F7	4F	24	35	C6	DC	94	-	BE	0F	A9	76	65	D5	C9	37
23	39	52	2D	35	31	75	60	-	56	A0	38	81	A8	F7	07	B1
5D	06	A4	AC	3D	DD	2D	0A	-	40	2C	7F	FE	2C	9C	26	22
89	86	60	60	36	89	08	16	-	C7	E9	E4	99	02	3F	7C	45
17	3C	5F	2A	2F	43	1A	2C	-	E3	81	BC	1F	19	59	68	FB

Elektronische Unterschrift: Beispiel 3

Testdatei: TEST.DAT - 24 Bytes

Inhalt: „Now is the time for all“ (ASCII)

4E	6F	77	20	69	73	20	74	(Hex)
68	65	20	74	69	6D	65	20	
66	6F	72	20	61	6C	6C	20	

Hashfunktion: AR/DFP

k1:	90	26	28	CB	EC	46	15	43
k2:	2A	41	52	2F	44	46	50	2A

768-Bit RSA Schlüssel 1

Modulus:

BC	7B	DC	71	12	56	E8	BD	-	B4	A0	CA	EB	B5	DB	B2	ED
CD	5F	78	70	29	A8	E6	AD	-	84	84	A1	D1	E8	C9	E1	2D
A0	2F	4B	70	AC	06	84	7C	-	35	D1	0E	79	4E	C6	E9	0D
43	70	62	AE	66	4B	A1	C8	-	05	00	F1	AD	7C	69	C6	23
0C	47	6E	C5	86	3B	40	F8	-	4A	76	06	AD	79	32	1C	4F
10	9F	87	C6	52	45	03	3F	-	2A	8B	A0	6E	21	91	13	87

Öffentlicher Exponent:

01 00 01

Geheimer Exponent:

08	A2	7A	A8	7F	6E	40	7E	-	A3	03	69	68	6A	4E	0F	4B
64	F3	86	61	4A	61	F4	CC	-	BC	31	15	7F	62	27	BA	CB
76	A1	7E	B3	97	08	91	67	-	33	51	49	78	20	8B	63	07
36	E0	CC	52	0F	D2	08	27	-	7B	6B	C5	FD	A1	39	41	1C
90	D9	93	B8	C5	18	48	06	-	FA	2C	49	EC	42	09	1C	F8
5E	86	C1	8A	47	0A	ED	3F	-	81	1E	57	95	A1	5E	5D	71

Hashwert:

5C	2D	EB	15	8B	52	4D	2A	-	BB	AB	A0	26	3B	4E	64	EA
----	----	----	----	----	----	----	----	---	----	----	----	----	----	----	----	----

Elektronische Unterschrift:

BA	4A	E8	A9	8C	8D	7F	73	-	34	17	93	94	85	F1	7D	49
EA	56	0B	58	DC	5F	E8	37	-	60	A9	37	DF	88	72	AF	0F
15	0D	8A	F5	39	F6	17	F7	-	60	BD	4F	92	43	A4	08	9B
10	3C	47	6D	21	23	DA	16	-	DD	AB	1E	EA	2A	CC	18	9F
6B	7B	75	E3	35	E3	15	3E	-	D7	81	C4	F4	E4	87	6B	A9
A7	B6	BB	73	DA	9D	1B	F9	-	78	53	A8	FD	01	70	AE	20

Elektronische Unterschrift: Beispiel 4

Testdatei: 00548495.DTA - 3072 Bytes

Hashfunktion: AR/DFP

k1:	90	26	28	CB	EC	46	15	43
k2:	2A	41	52	2F	44	46	50	2A

768-Bit RSA Schlüssel 2

Modulus:

A7	F8	85	82	48	0A	C6	C0	-	44	CD	18	C6	4D	D5	3A	C8
FD	13	04	31	EE	47	1F	E4	-	70	97	E0	A3	E7	F4	BF	95
C7	C5	4C	D6	CA	7A	83	B2	-	EC	CC	8A	52	89	4D	FE	A1
A5	1A	0D	CE	79	2D	38	D7	-	46	C1	00	95	35	D5	D5	84
DE	84	34	B3	FE	62	FA	AC	-	C5	29	63	C1	54	26	91	93
E4	FB	24	46	97	07	A8	91	-	FA	8A	FC	23	67	94	3B	65

Öffentlicher Exponent:

01 00 01

Geheimer Exponent:

4C	5A	51	61	FF	DA	7A	2F	-	02	F7	51	F8	2E	80	2B	59
1A	84	EE	E6	BD	7F	F2	34	-	D6	A3	8B	37	26	64	E0	43
B7	0B	EE	1A	42	EE	FE	F7	-	B1	E1	66	4D	0F	61	F7	49
09	A1	AF	55	2C	E2	8E	64	-	7F	56	25	4C	91	16	35	0F
D6	90	D9	BB	39	28	38	AB	-	86	71	64	F6	81	7A	50	AB
22	E1	E1	B4	E4	F2	E4	D9	-	8F	10	F9	6B	25	06	80	8F

Hashwert:

AA	05	85	78	F9	A2	F7	EE	-	FF	E7	F4	B0	35	19	83	0F
----	----	----	----	----	----	----	----	---	----	----	----	----	----	----	----	----

Elektronische Unterschrift:

29	69	5E	62	3D	DB	07	29	-	F3	9A	D1	C6	2A	5D	E6	66
36	13	C1	9D	69	62	45	6C	-	27	9B	D1	15	55	45	D1	DA
C0	98	06	4F	52	35	8F	F5	-	8A	A3	1D	B3	45	32	52	08
D5	6C	73	37	CA	65	0D	F6	-	8F	FC	00	3E	7B	15	18	D0
6D	B2	60	77	E5	62	67	44	-	94	CB	3C	22	8A	35	5A	27
10	72	D0	24	66	CD	28	4E	-	AC	1E	AA	7B	B2	8B	4C	D0

Elektronische Unterschrift: Beispiel 5

Testdatei: 00548495.ZKA - 1376 Bytes

Hashfunktion: AR/DFP

k1:	90	26	28	CB	EC	46	15	43
k2:	2A	41	52	2F	44	46	50	2A

768-Bit RSA Schlüssel 2

Modulus:

A7	F8	85	82	48	0A	C6	C0	-	44	CD	18	C6	4D	D5	3A	C8
FD	13	04	31	EE	47	1F	E4	-	70	97	E0	A3	E7	F4	BF	95
C7	C5	4C	D6	CA	7A	83	B2	-	EC	CC	8A	52	89	4D	FE	A1
A5	1A	0D	CE	79	2D	38	D7	-	46	C1	00	95	35	D5	D5	84
DE	84	34	B3	FE	62	FA	AC	-	C5	29	63	C1	54	26	91	93
E4	FB	24	46	97	07	A8	91	-	FA	8A	FC	23	67	94	3B	65

Öffentlicher Exponent:

01 00 01

Geheimer Exponent:

4C	5A	51	61	FF	DA	7A	2F	-	02	F7	51	F8	2E	80	2B	59
1A	84	EE	E6	BD	7F	F2	34	-	D6	A3	8B	37	26	64	E0	43
B7	0B	EE	1A	42	EE	FE	F7	-	B1	E1	66	4D	0F	61	F7	49
09	A1	AF	55	2C	E2	8E	64	-	7F	56	25	4C	91	16	35	0F
D6	90	D9	BB	39	28	38	AB	-	86	71	64	F6	81	7A	50	AB
22	E1	E1	B4	E4	F2	E4	D9	-	8F	10	F9	6B	25	06	80	8F

Hashwert:

0F	8E	CD	36	27	D8	49	16	-	C4	2C	65	D5	7A	8B	97	8A
----	----	----	----	----	----	----	----	---	----	----	----	----	----	----	----	----

Elektronische Unterschrift:

56	3B	1F	5F	0B	CF	31	85	-	F7	D7	6A	8D	21	64	66	69
6A	0D	85	72	64	F5	8C	E4	-	56	3C	85	7D	E2	AF	06	5F
06	37	47	BE	93	4F	D3	8C	-	EF	61	59	49	54	16	65	42
B9	C6	4E	15	2F	B5	F2	DF	-	CB	80	67	4F	F7	69	E7	21
89	64	3A	CA	14	37	21	30	-	2F	E0	1A	13	6D	B7	8D	49
98	11	BB	A6	57	59	DE	AD	-	0E	41	38	A3	7B	18	41	2F

Elektronische Unterschrift: Beispiel 6

Testdatei: TEST.DAT - 24 Bytes

Inhalt: „Now is the time for all“ (ASCII)

4E	6F	77	20	69	73	20	74	(Hex)
68	65	20	74	69	6D	65	20	
66	6F	72	20	61	6C	6C	20	

Hashfunktion: AR/DFP

k1:	90	26	28	CB	EC	46	15	43
k2:	2A	41	52	2F	44	46	50	2A

768-Bit RSA Schlüssel 2

Modulus:

A7	F8	85	82	48	0A	C6	C0	-	44	CD	18	C6	4D	D5	3A	C8
FD	13	04	31	EE	47	1F	E4	-	70	97	E0	A3	E7	F4	BF	95
C7	C5	4C	D6	CA	7A	83	B2	-	EC	CC	8A	52	89	4D	FE	A1
A5	1A	0D	CE	79	2D	38	D7	-	46	C1	00	95	35	D5	D5	84
DE	84	34	B3	FE	62	FA	AC	-	C5	29	63	C1	54	26	91	93
E4	FB	24	46	97	07	A8	91	-	FA	8A	FC	23	67	94	3B	65

Öffentlicher Exponent:

01 00 01

Geheimer Exponent:

4C	5A	51	61	FF	DA	7A	2F	-	02	F7	51	F8	2E	80	2B	59
1A	84	EE	E6	BD	7F	F2	34	-	D6	A3	8B	37	26	64	E0	43
B7	0B	EE	1A	42	EE	FE	F7	-	B1	E1	66	4D	0F	61	F7	49
09	A1	AF	55	2C	E2	8E	64	-	7F	56	25	4C	91	16	35	0F
D6	90	D9	BB	39	28	38	AB	-	86	71	64	F6	81	7A	50	AB
22	E1	E1	B4	E4	F2	E4	D9	-	8F	10	F9	6B	25	06	80	8F

Hashwert:

5C	2B	EB	15	8B	52	4D	2A	-	BB	AB	A0	26	3B	4E	64	EA
----	----	----	----	----	----	----	----	---	----	----	----	----	----	----	----	----

Elektronische Unterschrift:

9F	4D	F6	C9	8D	DE	93	68	-	F5	80	F4	27	0A	C7	90	67
4A	BD	15	75	E3	16	04	7A	-	C3	04	4E	E7	BC	75	11	66
F6	05	A0	37	27	1F	DC	12	-	A2	61	F2	5F	B7	24	86	CD
3E	A3	49	86	AF	4A	7C	18	-	5B	6E	68	15	4E	B0	9F	30
D4	36	30	30	A3	1E	8C	B0	-	74	F6	8C	FA	05	A1	6F	9F
D3	7E	72	2B	1A	E0	79	5C	-	A0	21	E2	C8	44	CD	94	2B

2.2.3 Elektronische Unterschrift der Version A004

Unter Beachtung der in Kapitel 2.2.1 genannten Anforderungen ist das nachfolgend beschriebene Verfahren für die Elektronische Unterschrift ab dem 1. April 2002 bankseitig verpflichtend zu unterstützen.

2.2.3.1 Einleitung

Die von der ZKA-Chipkarte bereitgestellten asymmetrischen kryptographischen Algorithmen basieren auf dem RSA-Algorithmus mit ungeraden öffentlichen Exponenten ([[RSA](#)]).

Im nachfolgenden Kapitel 2.2.3.2 „RSA-Schlüsselkomponenten“ werden das Konstruktionsprinzip und die **Schlüsselkomponenten** der öffentlichen und privaten RSA-Schlüssel gemäß Anhang B von [[EMV B2](#)], Anhang A von [[ISO DS2](#)] und [[PKCS1](#)] für ungerade öffentliche Exponenten erläutert.

Ein **Signatur-Algorithmus** besteht aus einem Algorithmus zur Signaturerzeugung und einem hierzu inversen Algorithmus zur Klartextrückgewinnung. Der als Standard von der ZKA-Chipkarte unterstützte Signatur-Algorithmus wird in Kapitel 2.2.3.3 unter „Signaturerzeugung“ beschrieben.

Der beschriebene Signatur-Algorithmus auf Basis des RSA-Algorithmus wird durch die ZKA-Chipkarte nur im Rahmen von Signaturverfahren eingesetzt. Ein **Signaturverfahren** legt fest, in welcher Weise eine Nachricht M zu einer Bytefolge aufzubereiten ist, die dann in die Signaturerzeugung eines Signatur-Algorithmus eingeht. Die durch ein Signaturverfahren erzeugte Bytefolge wird als **Digital Signature Input (DSI)** bezeichnet.

In Kapitel 2.2.3.4 „Signaturverfahren gemäß DIN-Spezifikation“ des vorliegenden Dokuments wird das Signaturverfahren beschrieben, das durch die für die ZKA-Chipkarte spezifizierte Signatur-Anwendung zur Erzeugung digitaler Signaturen unterstützt wird. Dieses Signaturverfahren entspricht der DIN-Spezifikation [[DINSIG](#)] einer Signatur-Anwendung/Funktion nach SigG und SigV.

2.2.3.2 RSA-Schlüsselkomponenten

Ein RSA-Schlüsselpaar besteht aus

- einem öffentlichen Schlüssel P_K und
- einem privaten Schlüssel S_K

Öffentlicher und privater Schlüssel bestehen aus **Schlüsselkomponenten**. RSA-Schlüssel werden auch als **asymmetrische Schlüssel** bezeichnet.

Zur Erzeugung eines RSA-Schlüsselpaares mit einem ungeraden **öffentlichen Exponenten e** werden zwei verschiedene **Primzahlen p und q (Primfaktoren)** verwendet, für die e teilerfremd zu $(p-1)$ und $(q-1)$ ist.

Der zugehörige **private Exponent d** ist dann bestimmt durch

$$e \cdot d \equiv 1 \pmod{\text{kgV}(p-1, q-1)}.$$

Die Primzahlen p und q sowie der private Exponent d müssen geheimgehalten werden.

Das Produkt der Primzahlen $n = p \cdot q$ wird als **Modulus** bezeichnet.

Der **öffentliche Schlüssel** P_K des RSA-Schlüsselpaares besteht aus den Komponenten

- Modulus n und
- öffentlicher Exponent e .

Der **private Schlüssel** S_K des RSA-Schlüsselpaares kann auf zwei Arten durch Komponenten dargestellt werden (vgl. [\[PKCS1\]](#)):

1. Darstellung von S_K durch die Komponenten:

- Modulus n und
- privater Exponent d ,

2. Darstellung von S_K durch die Komponenten:

- Primfaktor p ,
- Primfaktor q ,
- $d_p = d \bmod (p-1)$,
- $d_q = d \bmod (q-1)$ und
- $q_{\text{Inv}} = q^{-1} \bmod p$.

Nur die Komponente d der ersten Darstellung muss geheimgehalten werden. Die Komponenten der 2. Darstellung werden als **Chinese Remainder Theorem-Parameter (CRT-Parameter)** bezeichnet. Die CRT-Parameter müssen sämtlich geheimgehalten werden.

Die ZKA-Chipkarte unterstützt den RSA-Algorithmus mit beliebigen ungeraden öffentlichen Exponenten, die die Länge des Modulus nicht überschreiten. In der Regel wird der ungerade öffentliche Exponent $F_4 = 2^{16} + 1$ verwendet. In dem vorliegenden Dokument wird die folgende Notation verwendet:

k bezeichnet die Bit-Länge des Modulus n eines RSA-Schlüsselpaares.

k ist durch die Gleichung $2^{k-1} \leq n < 2^k$ eindeutig definiert.

n lässt sich darstellen als Folge von Bit

$$n = b_k b_{k-1} \dots b_1, \text{ wobei } b_k \neq 0 \text{ ist.}$$

Der Wert von n als ganzer Zahl wird dadurch bestimmt, dass das erste, linke Bit b_k das höchstwertige Bit und das letzte, rechte Bit b_1 das niedrigstwertige Bit in der Binärdarstellung von n ist.

Zu k existieren eindeutige Zahlen $N \geq 1$ und $8 \geq r \geq 1$ mit $k = 8 \cdot (N-1) + r$. Dann lässt sich n auch als Folge von Bit schreiben als

$$n = b_r b_{r-1} \dots b_1 b_{8 \cdot (N-1)} \dots b_{8 \cdot (N-2) + 1} \dots b_8 \dots b_1.$$

Wenn $r = 8$ ist, lässt sich n direkt als Folge von N Bytes schreiben:

$$n = B_N B_{N-1} \dots B_1, \text{ wobei } B_N \neq '00' \text{ und } B_N \geq '80' \text{ ist.}$$

Falls $r < 8$ ist, stellt man $8-r$ binäre 0 der Bitfolge $b_r b_{r-1} \dots b_1 b_{8*(N-1)} \dots b_{8*(N-2)+1} \dots b_8 \dots b_1$ voran:

$$n = 0 \dots 0 b_r b_{r-1} \dots b_1 b_{8*(N-1)} \dots b_{8*(N-2)+1} \dots b_8 \dots b_1.$$

und erhält wiederum eine Bytefolge

$$n = B_N B_{N-1} \dots B_1, \text{ wobei } B_N \neq '00' \text{ und } B_N < '80' \text{ ist.}$$

Der ganzzahlige Wert von n wird durch führende 0 in der Binärdarstellung nicht geändert, so dass die Darstellung von n als Folge von N Bytes den durch eine Folge von k Bit dargestellten Zahlwert unverändert lässt.

N ist die Byte-Länge von n.

Die ZKA-Chipkarte verwendet nur Moduli, die mindestens 128 Bytes lang sind. Aus technischen Gründen können durch die ZKA-Chipkarte

- für die Berechnung einer Signatur nur Moduli mit einer maximalen Länge von 256 Bytes und
- für die Prüfung einer Signatur nur Moduli mit einer maximalen Länge von 252 Bytes

verarbeitet werden.

2.2.3.3 Signatur-Algorithmus

Signaturerzeugung

Es sei S_K ein privater RSA-Schlüssel bestehend aus dem Modulus n und dem privaten Exponenten d oder bestehend aus den CRT-Parametern. Der zugehörige öffentliche RSA-Schlüssel P_K bestehe aus dem Modulus n und dem öffentlichen Exponenten e .

Dann können mit S_K binär kodierte Bytefolgen x signiert werden, deren sich aus der Binärdarstellung von x ergebender ganzzahliger Wert zwischen 0 und $n-1$ liegt. x lässt sich somit darstellen als Bytefolge mit einer Länge von N Bytes und als Bitfolge mit einer Länge von k Bit. Das k -te Bit in der darstellenden Byte- oder Bitfolge kann, muss aber nicht, den Wert 1 haben. Sofern vorhanden haben die Bit $b_{8*N} \dots b_{k+1}$ in der darstellenden Bytefolge den Wert 0.

Für die Signaturerzeugung mit dem aus n und d bestehenden privaten Schlüssel wird die folgende Notation verwendet:

$$\text{sign}(S_K)[x] = x^d \bmod n$$

Falls der private Schlüssel S_K aus den CRT-Parametern besteht, berechnet sich $\text{sign}(S_K)[x] = x^d \bmod n$ wie folgt:

$$\text{sign}(S_K)[x] = s_2 + h*q$$

wobei S_2 und h wie folgt berechnet werden:

$$\begin{aligned}s_1 &= x^{dp} \bmod p \\ s_2 &= x^{dq} \bmod q \\ h &= q \operatorname{Inv}(s_1 - s_2) \bmod p.\end{aligned}$$

Hierbei werden die Potenzierungen $x^d \bmod n$, $x^{dp} \bmod p$, $x^{dq} \bmod q$ mit der ganzen Zahl ausgeführt, deren Wert sich aus der Binärdarstellung von x ergibt.

Das Ergebnis der Signaturerzeugung ist wiederum eine Bytefolge s , die sich als Binärdarstellung des ganzzahligen Wertes der Potenz $x^d \bmod n$ bzw. von $s_2 + h \cdot q$ ergibt. Dieser ganzzahlige Wert liegt wieder zwischen 0 und $n-1$. s lässt sich somit darstellen als Bytefolge mit einer Länge von N Bytes und als Bitfolge mit einer Länge von k Bit. Das k -te Bit in der darstellenden Byte- oder Bitfolge kann, muss aber nicht, den Wert 1 haben. Sofern vorhanden haben die Bit $b_{8 \cdot N} \dots b_{k+1}$ in der darstellenden Bytefolge den Wert 0.

Klartextrückgewinnung

Es sei P_K ein öffentlicher RSA-Schlüssel bestehend aus dem Modulus n und dem öffentlichen Exponenten e .

Dann kann mit P_K aus einer binär kodierten Bytefolge s Klartext zurückgewonnen werden, wenn sich der sich aus der Binärdarstellung von s ergebende ganzzahlige Wert zwischen 0 und $n-1$ liegt. s lässt sich somit darstellen als Bytefolge mit einer Länge von N Bytes und als Bitfolge mit einer Länge von k Bit. Das k -te Bit in der darstellenden Byte- oder Bitfolge kann, muss aber nicht, den Wert 1 haben. Sofern vorhanden haben die Bit $b_{8 \cdot N} \dots b_{k+1}$ in der darstellenden Bytefolge den Wert 0.

Für die Klartextrückgewinnung wird die folgende Notation verwendet:

$$\operatorname{recover}(P_K)[s] = s^e \bmod n$$

Hierbei wird die Potenzierung $s^e \bmod n$ mit der ganzen Zahl ausgeführt, deren Wert sich aus der Binärdarstellung von s ergibt.

Das Ergebnis der Klartextrückgewinnung ist eine ganze Zahl, deren Wert zwischen 0 und $n-1$ liegt. Es lässt sich somit darstellen als Bytefolge mit einer Länge von N Bytes und als Bitfolge mit einer Länge von k Bit. Das k -te Bit in der darstellenden Byte- oder Bitfolge kann, muss aber nicht, den Wert 1 haben. Sofern vorhanden haben die Bit $b_{8 \cdot N} \dots b_{k+1}$ in der darstellenden Bytefolge den Wert 0.

Für ein RSA-Schlüsselpaar P_K und S_K gilt:

$$\operatorname{recover}(P_K)[\operatorname{sign}(S_K)[x]] = x$$

2.2.3.4 Signaturverfahren gemäß DIN-Spezifikation

Im Folgenden werden die in ein Signaturverfahren eingehenden Nachrichten M als Bitfolge der Bit-Länge m aufgefasst. Eine Nachricht lässt sich demnach schreiben als Folge von Bit b_i

$$M = b_m b_{m-1} \dots b_1$$

Wenn M als Binärzahl aufgefasst wird, ist das erste, linke Bit b_m das höchstwertige Bit und das letzte, rechte Bit b_1 das niedrigstwertige Bit. Das oder die höchstwertigen Bit einer Nach-

richt können den Wert 0 haben.

In der Regel ist m ein Vielfaches von 8, so dass sich M auch als Folge von Bytes darstellen lässt. Verfahren zur Kodierung von Nachrichten als Bit- oder Bytefolgen sind nicht Teil der durch die ZKA-Chipkarte unterstützten Signaturverfahren.

Falls ein Teil der zu signierenden Nachricht M als Bytefolge in dem DSI enthalten ist, kann dieser Teil durch die Klartextrückgewinnung des Signatur-Algorithmus aus der Signatur zurückgewonnen werden. In diesem Fall handelt es sich um ein Signaturverfahren **mit Nachrichtenrückgewinnung**. Der **zurückgewinnbare Teil** der Nachricht M wird als M_r bezeichnet. Falls die gesamte signierte Nachricht aus der Signatur zurückgewonnen werden kann, handelt es sich um **vollständige Nachrichtenrückgewinnung** ($M = M_r$), andernfalls um partielle Nachrichtenrückgewinnung. Der **nicht zurückgewinnbare Teil** der Nachricht M wird dann als M_n bezeichnet.

Falls der DSI keinen Teil der Nachricht als Bytefolge enthält, handelt es sich um ein Signaturverfahren **ohne Nachrichtenrückgewinnung** ($M = M_n$).

Zur Prüfung einer mit einem Signaturverfahren erzeugten digitalen Signatur wird außer der Signatur der nicht zurückgewinnbare Teil der signierten Nachricht benötigt.

Das im Folgenden beschriebene Signaturverfahren ist in [\[DINSIG\]](#) spezifiziert. Es ist ein Signaturverfahren ohne Nachrichtenrückgewinnung, das auf [\[ISO DS2\]](#) basiert. Es verwendet zur Erzeugung des DSI

- einen Hash-Algorithmus und
- einen Format-Mechanismus.

Ein Hash-Algorithmus bildet Bitfolgen beliebiger Länge (**Eingabe-Bitfolgen**) auf Bytefolgen einer festen, durch den Hash-Algorithmus festgelegten Länge ab. Das Ergebnis der Anwendung eines Hash-Algorithmus auf eine Bitfolge wird als **Hash-Wert** bezeichnet.

Das durch die für die ZKA-Chipkarte spezifizierte Signatur-Anwendung zur Erzeugung digitaler Signaturen unterstützte Signaturverfahren verwendet den Hash-Algorithmus **RIPEMD-160**.

Der Hash-Algorithmus RIPEMD-160 ist in [\[RIPEMD\]](#) und [\[ISO HF3\]](#) spezifiziert. RIPEMD-160 bildet Eingabe-Bitfolgen beliebiger Länge auf einen als Bytefolge dargestellten Hash-Wert von 20 Bytes Länge ab. Teil des Hash-Algorithmus ist das Padding von Eingabe-Bitfolgen auf ein Vielfaches von 64 Bytes. Das Padding erfolgt auch dann, wenn die Eingabe-Bitfolge bereits eine Länge hat, die ein Vielfaches von 64 Bytes ist.

RIPEMD-160 verarbeitet die Eingabe-Bitfolgen in Blöcken von 64 Bytes Länge.

Der Hash-Wert einer Eingabe-Bitfolge x unter dem Hash-Algorithmus RIPEMD-160 wird wie folgt bezeichnet:

RIPEMD(x).

Im Folgenden wird der Format-Mechanismus des Signaturverfahrens gemäß Spezifikation [\[DINSIG\]](#) beschrieben. Die verwendeten Abkürzungen sind in Kapitel 2.2.3.2 „RSA-Schlüsselkomponenten“ definiert.

Berechnen einer Signatur

Die folgenden Schritte werden gemäß Spezifikation [\[DINSIG\]](#) und [\[ISO DS2\]](#) zum Berechnen einer Signatur zu der Nachricht M der Bit-Länge m ausgeführt.

- Der Hash-Wert RIPEMD(M) mit einer Länge von 160 Bit wird berechnet. Hierbei gehen betriebssystemabhängige Zeichen (*bei Windows CR, LF, CRLF und Control-Z*) in die Bildung des Hashwertes nicht ein.
- Der DSI wird erzeugt.
Der DSI ist eine Folge von k Bit, der wie folgt aufgebaut ist:

Bezeichnung	Bit-Länge	Wert
Header	2	0 1
More-Data-Bit	1	1, da $M = M_n$ ist
Paddingfeld	k-235	k-236 Bit 0, gefolgt von einem Bit 1 (Grenzbit)
Datenfeld	64	Zufallszahl: Die Zufallszahl muss bei jeder Signaturberechnung dynamisch erzeugt und in den DSI eingestellt werden.
Hash-Wert	160	RIPEMD(M)
Trailer	8	'BC'

Die Nachricht M besteht komplett aus dem nicht zurückgewinnbaren Teil M_n .
Die ersten vier Bit des DSI können nur den Wert '6' annehmen, da $k-236 > 0$ ist.

- Aus dem DSI wird mit dem Algorithmus zur Signaturerzeugung gemäß Kapitel 2.2.3.3 „Signatur-Algorithmus“ eine Signatur berechnet.

Hierbei ist zu beachten, dass der DSI als Folge von k Bit darstellbar ist, wobei das erste (höchstwertige) Bit den Wert 0 hat. Der sich aus der Binärdarstellung ergebende ganzzahlige Wert des DSI ist damit kleiner als 2^{k-1} und damit kleiner als der Wert des Modulus n.

Ferner lässt sich der DSI als Bytefolge darstellen, ggf. indem maximal 7 Bit mit dem Wert 0 dem ersten Bit der Bitfolge vorangestellt werden. Diese Bytefolge hat den selben ganzzahligen Wert wie die den DSI darstellende Bitfolge.

Die Signatur ist als Bytefolge darstellbar, deren Byte-Länge höchstens N ist. In der Darstellung des Modulus n als Bytefolge hat das Bit b_k den Wert 1 und die Bit $b_{8 \cdot N} b_{8 \cdot N - 1} \dots b_{k+1}$ haben, sofern vorhanden, den Wert 0. In der Darstellung der Signatur als Bytefolge haben die Bit $b_{8 \cdot N} b_{8 \cdot N - 1} \dots b_{k+1}$ ebenfalls den Wert 0.

Prüfen einer Signatur

Die folgenden Schritte werden gemäß Spezifikationen [\[DINSIG\]](#) und [\[ISO DS2\]](#) zum Prüfen einer Signatur ausgeführt. Hierzu müssen die zu prüfende Signatur s und die Nachricht M' der Bit-Länge m' vorliegen.

- Die Signatur muss als Bytefolge darstellbar sein, deren Byte-Länge höchstens N ist. In der Darstellung von s als Bytefolge müssen die Bit $b_{8 \cdot N} b_{8 \cdot N - 1} \dots b_{k+1}$, sofern vorhanden den Wert 0 haben. Ist das nicht der Fall, wird die Signatur abgewiesen.
Der sich aus der Binärdarstellung von s ergebende ganzzahlige Wert muss zwischen 0 und n-1 liegen. Ist das nicht der Fall, wird die Signatur abgewiesen.
- Auf die Signatur wird der Algorithmus zur Klartextrückgewinnung gemäß Kapitel 2.2.3.3 „Signatur-Algorithmus“ angewandt. Das Ergebnis ist eine Bitfolge $b_k \dots b_1$, die als DSI'

bezeichnet wird. DSI' muss den folgenden Anforderungen genügen:

Das niedrigstwertige Byte bestehend aus $b_8 \dots b_1$ hat den Wert 'BC'.

Das Bit b_{k-1} hat den Wert 1 und alle höherwertigen Bit haben den Wert 0.

Das Bit b_{k-2} („More Data“-Bit) hat den Wert 1.

Das Paddingfeld besteht aus $(k - 236)$ Nullen und einer 1 (Grenzbit).

Sind die Anforderungen nicht erfüllt, wird die Signatur abgewiesen.

- Aus dem DSI' wird ein Hash-Wert' entnommen. Der Hash-Wert' besteht aus den 160 Bit, die dem Trailer 'BC' vorausgehen.
- Der Hash-Wert RIPEMD(M') wird berechnet und mit dem Hash-Wert' verglichen. Falls die Werte gleich sind, war die Prüfung der Signatur erfolgreich. Andernfalls wird die Signatur abgelehnt.

Notation

Für die Berechnung einer Signatur zu einer Nachricht M mit dem Signaturverfahren gemäß [DINSIG], dem Signatur-Algorithmus RSA und dem privaten RSA-Schlüssel S_K wird die folgende Notation verwendet:

$\text{sign}_{\text{DINSIG}}(S_K)[M]$.

Für die Prüfung einer Signatur s zu einer Nachricht M mit dem Signaturverfahren gemäß [DINSIG], dem Signatur-Algorithmus RSA und dem öffentlichen RSA-Schlüssel P_K wird die folgende Notation verwendet:

$\text{verify}_{\text{DINSIG}}(P_K)[s, M]$.

2.2.3.5 Referenzen

- [DINSIG] DIN-Spezifikation der Schnittstelle zu Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, DIN NI-17.4, Version 1.0, 15.12.1998
- [EMV B2] EMV2000, Integrated Circuit Card Specification for Payment Systems, Book 2, Security and Key Management, Version 4.0, EMVCo, December 2000
- [ISO DS2] ISO 9796 - 2, Information technology - Security techniques - Digital signature scheme giving message recovery, Part 2: Mechanisms using a hash function, 1997
- [ISO HF3] ISO 10118 - 3, Information technology - Security techniques - Hash-functions, Part 3: Dedicated hash functions, 1998
- [PKCS1] PKCS #1: RSA Cryptography Standard, Version 2.0, 1.10.1998
- [RIPEMD] H. Dobbertin, A. Bosselaers, B. Preneel, RIPEMD-160: A strengthened version of RIPEMD, 1996
- [RSA] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, vol. 21, n. 2, 1978, 120-126

2.2.3.6 Signaturformat der ZKA-Chipkarte bei DFÜ mit Kunden

Ausgangslage

Es ist geplant, zukünftig in allen kreditwirtschaftlichen Verfahren die ZKA-Signaturkarte als Sicherheitsmedium für die Generierung von elektronischen Unterschriften einzusetzen.

Die vorliegende Spezifikation für die Elektronische Unterschrift A004 beschreibt dazu das zukünftig mit Einführung der Version A004 im DFÜ-Verfahren einzusetzende, anwendungsunabhängige Signaturformat der ZKA-Chipkarte. Darüber hinaus wird die Belegung der Felder in der EU-Datei sowie der Aufbau des Initialisierungsbriefes festgelegt.

Signaturformat

Die Version A004 der Elektronischen Unterschrift basiert auf RSA-Signaturen, die mit Schlüsseln generiert werden, deren Moduli eine Länge von 1024 Bit haben. Die ZKA-Chipkarte unterstützt den RSA-Algorithmus mit beliebigen ungeraden öffentlichen Exponenten. In der Regel wird der ungerade öffentliche Exponent $F_4 = 2^{16} + 1$ verwendet. Als Paddingformat wird das in der „DIN-Spezifikation der Schnittstelle zu Chipkarten mit digitaler Signatur-Anwendung/Funktion nach SigG und SigV“ beschriebene Paddingformat „ISO 9796 Part 2 mit Zufallszahl“ verwendet.

Ermittlung des Hash-Wertes über die zu unterschreibende Datei

Das in der Version A004 der Elektronischen Unterschrift durch die ZKA-Chipkarte unterstützte Signaturverfahren verwendet den Hash-Algorithmus RIPEMD-160.

RIPEMD-160 bildet Eingabe-Bitfolgen beliebiger Länge auf einen als Bytefolge dargestellten Hash-Wert von 20 Bytes Länge ab. Teil des Hash-Algorithmus ist das Padding von Eingabe-Bitfolgen auf ein Vielfaches von 64 Bytes. Das Padding erfolgt auch dann, wenn die Eingabe-Bitfolge bereits eine Länge hat, die ein Vielfaches von 64 Bytes ist. RIPEMD-160 verarbeitet die Eingabe-Bitfolgen in Blöcken von 64 Bytes Länge. Das Padding der Nachricht auf die entsprechende Blockgröße wird in der Beschreibung des Hashverfahrens spezifiziert. Der zu verwendende Initialisierungsvektor ist ebenfalls in der Beschreibung des Hashverfahrens festgelegt.

Der im Initialisierungsbrief angegebene Hashwert wird ebenfalls nach diesem Verfahren über die 256 Bytes – bestehend aus öffentlichem Exponenten und Modulus – berechnet.

Aufbau der Unterschriftsdatei

Vor dem Versand einer Elektronischen Unterschrift wird diese in eine separat zu übertragende Unterschriftsdatei eingestellt, die den folgenden Aufbau hat:

Inhalt	Länge in Bytes	Daten-format ²⁴	Belegung	Erläuterung
Versionsnummer	4	an	„A004“	
Länge des Modulus	4	n	„1024“	
Auftragsart	3	an	z.B. 'IZV'	Auftragskürzel der Originaldatei
EU	128	binär	'0, ..., 0, SIGNATUR'	rechtsbündig
User-ID	8	an	z.B. 'A2B2C2D2'	
Originaldatei	128	an		Lokaler Dateiname der Originaldatei ²⁵
Datum/Uhrzeit	16	an	jjjjmmmtX'20'hhmmssX'20'	
Datum/Uhrzeit	16	an	jjjjmmmtX'20'hhmmssX'20'	
Frei nutzbares Feld	8	binär	X'00'	Zur Zeit nicht benutzt
Reserve	197	binär	X'00'	Zur Zeit nicht benutzt

Der Aufbau der Unterschriftsdatei ist für die EU-Versionen A003 und A004 identisch (vergl. Kapitel 2.2.2.5 „Formate“)

²⁴ an = alphanummerisch; n = numerisch; Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Werte im Binär-Format werden rechtsbündig eingestellt und links mit X'00' aufgefüllt.

²⁵ Bei EDIFACT ist der lokale Dateiname der Originaldatei – im Gegensatz zu BCS – wie folgt strukturiert:

35 Bytes	SenderID (linksbündig, rechts mit X'20' auffüllen)
58 Bytes	Interchange Control Reference (Linksbündig, rechts mit X'20' auffüllen)
35 Bytes	EmpfängerID (linksbündig, rechts mit X'20' auffüllen)

DFÜ – Abkommen

Anlage 2 (Standards für die Sicherheit)

Beispiel für einen INI-Brief DFÜ (A004)

Benutzername	system	Kundensoftware-interner Name (Angabe freigestellt)
Datum	TT.MM.JJJJ	Datum der Erstellung des Initialisierungs- bzw. Public-Key-Änderungsauftrages
Uhrzeit	HH:MM	Uhrzeit der Erstellung des Initialisierungs- bzw. Public-Key-Änderungsauftrages
Empfänger	DFÜ-Bank	Hostname der Bank (max. 8 Stellen; wird von der jeweiligen Bank mitgeteilt)
User-ID	xxxxxxx	(8 Bytes alphanummerisch; beginnend mit einem Alphazeichen; wird von der jeweiligen Bank mitgeteilt)
Kunden-ID	yyyyyyy	(8 Bytes alphanummerisch; wird von der jeweiligen Bank mitgeteilt)
EU-Version	A004	

Öffentlicher Schlüssel (Public-Key) für die Elektronische Unterschrift:

Exponent	1024															
	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

Modulo	1024															
	FF	12	03	26	E6	30	90	A5	06	01	EF	16	10	21	EE	D4
	77	23	27	A9	14	17	07	F1	71	25	22	D5	91	00	41	0A
	D7	4A	2F	D5	6C	16	4E	C3	2D	82	F3	02	31	CD	FF	FB
	45	77	E4	7E	E5	B2	CB	7B	9A	5F	75	7B	32	7C	16	E5
	FB	16	41	0B	4A	39	0F	50	47	68	9C	9B	27	D2	A0	9C
	CA	23	A8	C3	1C	AB	A5	ED	72	75	9D	0A	B8	9B	37	BA
	00	CB	68	BB	AC	C8	D1	C8	D3	35	C8	BF	1F	A3	06	CF
	24	5A	DC	EB	84	64	86	D0	97	8F	E4	67	08	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 Unterschrift.

Ort / Datum	Firma / Name	Unterschrift
-------------	--------------	--------------

2.2.3.7 Testdaten Elektronische Unterschrift

Testdaten werden nachgereicht

2.3 Verschlüsselung

2.3.1 Allgemeine Anforderungen

Kunde und Kreditinstitut vereinbaren, welche Daten von der Bank verschlüsselt bereitgestellt werden sollen. Das Verschlüsselungsverfahren muss in jedem Fall der nachfolgenden Spezifikation entsprechen. Die konkrete technische Lösung muss für die gängigen Betriebssysteme, die beim Unterzeichner bzw. Empfänger zum Einsatz kommen können, kompatibel einsetzbar sein.

2.3.2 Schaffung der Voraussetzungen für die verschlüsselte Kommunikation

Bei dem zur Verschlüsselung eingesetzten Verfahren handelt es sich um ein **hybridisches Verfahren**, in dem der Kunde bei der Vorbereitung des Public-Key-Austausches die VPK-Datei dem Kreditinstitut zur Verfügung stellen muss.

Der Kunde überträgt die VPK-Datei an das Kreditinstitut mittels DFÜ. Zur Autorisierung gegenüber der Bank stehen dem Kunden zwei Möglichkeiten zur Verfügung:

- Signieren der VPK-Datei mittels Elektronischer Unterschrift. Dazu muss das Verfahren der Elektronischen Unterschrift beim Kunden bereits initialisiert sein.
- Generierung des INI-Briefes und Versand der VPK-Datei und des INI-Briefes zum Kreditinstitut.

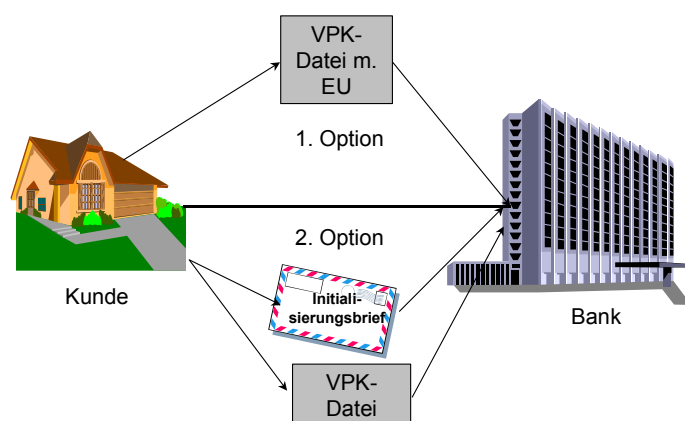


Abbildung 2.2: Generierung und Versand des INI-Briefes/ VPK-Datei zum Kreditinstitut

2.3.3 Vorbereitung der Verschlüsselung / Public-Key-Austausch

Als Voraussetzung für die Datenverschlüsselung muss der jeweilige Empfänger der verschlüsselten Daten dem Sender dieser Daten den öffentlichen Schlüssel seines RSA-

DFÜ – Abkommen

Anlage 2 (Standards für die Sicherheit)

Verschlüsselungs-Key-Paars bekannt machen.

Im Rahmen der Kunde-Bank-Beziehung übermittelt der Kunde seinen Verschlüsselungs-Public-Key unter Nutzung der neu einzuführenden Auftragsart „**VPK**“ (= **V**erschlüsselungs-**P**ublic-Key-**K**unde) mit folgender Datei:

Inhalt der VPK-Datei	Länge in Bytes ²⁶	Erläuterung/Belegung
Versionsnummer	4 ASCII	‚V001‘
Verschlüsselungsverfahren	2 ASCII	‚03‘ (=Triple DES mit zwei 64 Bit Schlüsseln)
Kunden-ID	8 ASCII	z.B. ‚A1B1C1D1‘
Länge Exponent	4 ASCII	‚0768‘
Exponent	128 binär	00 ... 01 00 00 00 0F(Hex) (siehe Kapitel 2.3.6.3 „Exponent“). Gegebenenfalls können auch variable Werte für den Exponenten verwendet werden oder die 4. Fermat'sche Primzahl. Es ist sicherzustellen, dass nicht der schwache Exponent 3 verwendet wird.
Länge Modulo	4 ASCII	‚0768‘
Modulo	128 binär	Siehe Kapitel 2.3.6.4 „Modulo“
Hash-Wert des Public Keys	16 binär	Hashwertbildung gemäß Kapitel 2.2.2.2 „Definitionen“
Verwendung	2 ASCII	‚05‘ (=nur für Verschlüsselung)
Zeitstempel der Key-Generierung	20 ASCII	Format: ‚TT.MM.JJJJ,X'20'HH:MM:SS‘ (Datum/Uhrzeit)
Reserve	196 ASCII	Auffüllen mit X'20‘
EU-Datei gemäß Kapitel 2.2 „Kryptographische Verfahren ...“	512 binär	Feld wird nur angehängt, wenn Legitimation mit Elektronischer Unterschrift stattfindet ²⁷

Wenn die Legitimierung des VPK-Auftrages mit der Elektronischen Unterschrift durchgeführt wird, so wird die obige VPK-Datei und die zugehörige Unterschriftsdatei verknüpft und als eine Datei übertragen. Gleichzeitig wird der FTAM-Remote-Filename um die User-ID desjenigen erweitert, der die Elektronische Unterschrift generiert hat. Die User-ID wird in alphanumerisch mit der führenden Kennung „U“ als Auftragsparameter übergeben.

Der bankseitige Verschlüsselungs-Public-Key wird dem Kunden mit der nachfolgend dargestellten Datei - falls die Übermittlung im Wege der Datenfernübertragung erfolgt - unter Nutzung der neu einzuführenden Auftragsart „**VPB**“ (**V**erschlüsselungs-**P**ublic-Key-**B**ank) zur Verfügung gestellt.

²⁶ an = alphanummerisch; n = numerisch. Alphanummerische Felder werden linksbündig angeordnet und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt. Werte im Binär-Format werden rechtsbündig eingestellt und links mit X'00' aufgefüllt.

²⁷ Sofern die Autorisierung dieser Verschlüsselungs-Public-Key-Datei mit der Elektronischen Unterschrift stattfindet (alternativ ist die Legitimation per Initialisierungsbrief vorgesehen), wird die VPK-Datei um die entsprechende, nach dem in Kapitel 2 beschriebenen Verfahren für die Elektronische Unterschrift erstellte EU-Datei erweitert. In diesem Fall wird das Auftragsattribut „Dateiart“ im FTAM-Remote-Filename mit „B“ (= Original- und EU-Datei in einer physikalischen Datei) belegt. Im Falle des Versands eines Initialisierungsbriefes wird dieses Attribut auf „D“ gesetzt.

DFÜ – Abkommen

Anlage 2 (Standards für die Sicherheit)

Inhalt der VPB-Datei	Länge in Bytes ²⁸	Erläuterung/Belegung
Versionsnummer	4 ASCII	,V001'
Host-ID	8 ASCII	z.B. 'A3B3C3D3'
Länge Exponent	4 ASCII	'0768'
Exponent	128 binär	00 ... 01 00 00 00 0F(Hex) (siehe Kapitel 2.3.6.3 „Exponent“). Gegebenenfalls können auch variable Werte für den Exponenten verwendet werden oder die 4. Fermat'sche Primzahl. Es ist sicherzustellen, dass nicht der schwache Exponent 3 verwendet wird.
Länge Modulo	4 ASCII	'0768'
Modulo	128 binär	Siehe Kapitel 2.3.6.4 "Modulo"
Hash-Wert des Public Keys	16 binär	Hashwertbildung gemäß Kapitel 2.2.2.2 „Definitionen“
Verwendung	2 ASCII	'05' (=nur für Verschlüsselung)
Reserve	196 ASCII	Auffüllen mit X'20'

²⁸ Alphanummerische Felder werden linksbündig angeordnet und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt. Werte im Binär-Format werden rechtsbündig eingestellt und links mit X'00' aufgefüllt.

2.3.4 Ver- und Entschlüsselung

2.3.4.1 Vorgänge beim Sender

Generierung des geheimen DES-Schlüssels (2-Key-Triple-DES)

Es werden zwei zufällige Bitstrings **DEK_{left}** und **DEK_{right}** mit jeweils einer Länge von 64 Bit generiert. Die Verknüpfung von DEK_{left} und DEK_{right} wird als DEK bezeichnet.

Es sei

$$\text{DEK} = \text{DEK}_{\text{left}} || \text{DEK}_{\text{right}} = x_{127}, \dots, x_0$$

mit $\text{DEK}_{\text{left}} = x_{127}, \dots, x_{64}$ und $\text{DEK}_{\text{right}} = x_{63}, \dots, x_0$.

Bei der Interpretation der DES-Keys als natürliche Zahl wird angenommen, dass das jeweils linke Bit (x_{127} bzw. x_{63}) der Schlüssel als höchstwertigstes Bit der Zahl aufgefaßt wird.

Prüfen der geheimen DES-Schlüssel

Die generierten Zufallszahlen, die als rechte und linke Schlüsselhälfte des 2-Key-Triple-DES verwendet werden, sind daraufhin zu überprüfen, dass es sich nicht um einen schwachen oder halbschwachen DES-Schlüssel handelt

Die schwachen Schlüssel des DES							
01	01	01	01	01	01	01	01
FE	FE	FE	FE	FE	FE	FE	FE
1F	1F	1F	1F	0E	0E	0E	0E
E0	E0	E0	E0	F1	F1	F1	F1
Die halbschwachen Schlüssel des DES							
01	FE	01	FE	01	FE	01	FE
FE	01	FE	01	FE	01	FE	01
1F	E0	1F	E0	0E	F1	0E	F1
E0	1F	E0	1F	F1	0E	F1	0E
01	E0	01	E0	01	F1	01	F1
E0	01	E0	01	F1	01	F1	01
1F	FE	1F	FE	0E	FE	0E	FE
FE	1F	FE	1F	FE	0E	FE	0E
01	1F	01	1F	01	0E	01	0E
1F	01	1F	01	0E	01	0E	01
E0	FE	E0	FE	F1	FE	F1	FE
FE	E0	FE	E0	FE	F1	FE	F1

Vorbereitung zur Verschlüsselung von DEK

Der als natürliche Zahl interpretierte 128 Bit DEK wird vor dem höchstwertigsten Bit mit Nullbits auf 768 Bit aufgefüllt. Das Ergebnis heißt **PDEK** (siehe Kapitel 2.3.6.1 „PDEK“).

Verschlüsselung des geheimen DES-Schlüssels

PDEK wird anschließend mit dem öffentlichen Schlüssel des RSA-Schlüsselsystems des Empfängers verschlüsselt und anschließend mit führenden Nullbits auf 1024 Bit erweitert.

Das Ergebnis heißt **EDEK** (siehe Kapitel 2.3.6.2 „EDEK“). Es muss sichergestellt sein, dass EDEK ungleich DEK ist.

Verschlüsselung der Nachrichten

Padding der Nachricht:

Für das Padding der Nachricht wird die Methode **Padding with Octets** nach ANSI X9.23 angewendet, d. h. es werden in jedem Fall Daten an die zu verschlüsselnde Nachricht angefügt.

Anwendung des Verschlüsselungsalgorithmus:

Die Nachricht wird mit dem geheimen Schlüssel DEK nach dem 2-Key-Triple-DES-Verfahren, wie im ANSI X3.92-1981 spezifiziert, im CBC-Mode gemäß ANSI X3.106 verschlüsselt.

Hierbei wird folgender Initialisierungswert „ICV“ verwendet: X '00 00 00 00 00 00 00 00'.

Übermittlung

An den Kommunikationspartner wird der verschlüsselte 2-Key-Triple-DES-Schlüssel (bestehend aus DEK_{left} und DEK_{right}) (=EDEK) in einem der verschlüsselten Nachricht vorangestellten Vorsatz 'V' übertragen. Die zur Übertragung kommende Datei hat damit insgesamt folgenden Aufbau:

Feld	Inhalt	Länge in Bytes ²⁹	Erläuterung/Belegung
1	Satzart	1 an	'V'
2	Versionsnummer	3 an	Derzeit '001'
3	Vorsatzlänge	4 n	'0256'
4	Absender-ID	8 an	Bei Sendeauftrag des Kunden: Kunden-ID (z.B. 'A1B2C3D4') Bei Abholauftrag des Kunden: Host-ID (z.B. 'BANKABCD')
5	Empfänger-ID	8 an	Bei Sendeauftrag des Kunden: Host-ID (z.B. 'BANKABCD') Bei Abholauftrag des Kunden: Kunden-ID (z.B. 'A1B2C3D4')

²⁹ an = alphanummerisch; n = numerisch. Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt. Werte im Binär-Format werden rechtsbündig eingestellt und links mit X'00' aufgefüllt.

Feld	Inhalt	Länge in Bytes ²⁹	Erläuterung/Belegung
6	Verschlüsselter DEK (EDEK)	128 binär	Siehe Kapitel 2.3.6.2 "EDEK"
7	Hashwert des Verschlüsselungs-Public-Keys des Empfängers	16 binär	Bei Sendeauftrag des Kunden: Hashwert des VPB Bei Abholauftrag des Kunden: Hashwert des VPK (Hashwertbildung gemäß Kapitel 2.2.2.2 „Definitionen“)
8	Reserve	88 an	Zur Zeit nicht genutzt, X'20'

Nach dem Vorsatz folgt die verschlüsselte Nachricht

Feld	Inhalt	Länge in Bytes	Erläuterung/Belegung
9	Verschlüsselte Nachricht	binär variabel	Mit DEK verschlüsselte Originalnachricht

Zusätzlich wird der FTAM-Remote-Filename um den obigen Hashwert des Verschlüsselungs-Public-Keys des Empfängers im Feld „Auftragsparameter“ erweitert. Dieser Hashwert (16 Bytes binär) wird als ASCII-Text in hexadezimaler Schreibweise mit der führenden Kennung „H“ übergeben. Die Länge des Feldes Auftragsparameter im FTAM-Remote-Filename muss daher um 33 Bytes erweitert werden.

2.3.4.2 Vorgänge beim Empfänger

Prüfen des Hashwertes des Verschlüsselungs-Public-Keys

Der im FTAM-Remote-Filename übergebene Hashwert des Verschlüsselungs-Public-Keys des Empfängers wird mit dem empfängerseitig hinterlegten Hashwert verglichen. Anhand des Vergleichs wird die Aktualität des Verschlüsselungscodes des Senders überprüft. Wurde ein unzulässiger Hashwert empfangen, so wird die FTAM-Kommunikation beendet.

Handelt es sich beim Empfänger um die Bank, so werden folgende Antwortcodes³⁰ generiert, die kundenseitig die entsprechend beschriebenen Reaktionen auslösen, sofern im FTAM-Remote-Filename die Versionskennung des Anwendungsprotokolls „A3“ verwendet wird:

³⁰ Weitere für andere Zwecke reservierte Antwortcodes sind dem Kapitel 2.3.6 „Interne Datenformate der Funktion „Verschlüsselung““ zu entnehmen.

Antwortcode	Bemerkung
51	Verschlüsselungscode mit Bank muss aktualisiert werden. Auf dem Banksystem wurde ein neuer Verschlüsselungs-Public-Key generiert, der vom Kundensystem abgeholt werden muss. Der Anwender wird hierüber durch eine entsprechende Meldung hingewiesen. Solange der neue Verschlüsselungs-Public-Key bei der Bank noch nicht abgeholt wurde, kann der Kunde keine (verschlüsselten) Dateien an die Bank übermitteln. Der Antwortcode 51 kann auch dann vom Banksystem zurückgeliefert werden, wenn der im FTAM-Remote-Filename der verschlüsselten Datei eingestellte Hashwert des verwendeten Verschlüsselungs-Public-Keys der Bank (VPB) nicht mit dem bankseitig erwarteten Hashwert übereinstimmt. In diesem Fall muss der Kunde ebenfalls einen neuen Verschlüsselungs-Public-Key bei der Bank abholen.
54	Verschlüsselungscode muss neu verschickt werden. Kundenseitig wird nach erfolgreichem Versand des VPK-Auftrages und des dazugehörigen Legitimationsauftrages zunächst davon ausgegangen, dass die entsprechende Authentifizierung bei der Bank mit positivem Ergebnis durchgeführt wurde. Verläuft die bankseitige Unterschriftsprüfung der VPK-Datei jedoch negativ, so erhält das Kundensystem beim Abholversuch von verschlüsselt vereinbarten Auftragsarten den obigen Antwortcode 54.
56	Verschlüsselungscode noch nicht freigegeben. Solange der kundenseitige Verschlüsselungs-Public-Key bankseitig noch nicht authentifiziert wurde, erhält der Kunde bei dem Versuch, Daten mit den Auftragsarten abzuholen, für die die Verschlüsselung mit der Bank vereinbart wurde, den Returncode 56 „Verschlüsselungscode noch nicht freigegeben“.

Entschlüsselung des DES-Schlüssels

Die führenden 256 Nullbits des EDEK werden entfernt und die verbleibenden 768 Bit mit dem geheimen Schlüssel des RSA-Schlüsselsystems des Empfängers entschlüsselt. Anschließend liegt PDEK vor. Aus den niederwertigsten 128 Bits von PDEK erhält man den geheimen DES-Schlüssel DEK, der in die Einzelschlüssel DEK_{left} und DEK_{right} aufgesplittet wird.

Entschlüsselung der Nachricht

Mit dem geheimen DES-Schlüssel (bestehend aus DEK_{left} und DEK_{right}) wird die verschlüsselte Originalnachricht nach dem 2-Key-Triple-DES-Verfahren im CBC-Mode entschlüsselt. Hierbei wird wiederum der Initialisierungswert ICV (siehe Kapitel 2.3.6.1 „PDEK“) verwendet.

Entfernen der Paddinginformationen

Für das Entfernen der Paddinginformationen aus der entschlüsselten Nachricht wird die Methode „Padding with Octets“ nach ANSI X9.23 angewendet. Anschließend liegt die Originalnachricht unverschlüsselt vor.

2.3.5 Beispielhafte Beschreibung der Abläufe

Beispielparameter

Im Folgenden werden die Anwendungen dieser Funktionen anhand eines Beispiels mit folgenden Parametern beschrieben:

Parameter	Wert
Kunden-ID	'A1B1C1D1' (8-stellig, alphanummerisch)
User-ID	'A2B2C2D2' (8-stellig, alphanummerisch)
Auftragsart Originaldatei	'TST'
Auftragsart Unterschrift	'TST'
Auftragsnummern	'A000'
FTAM spezifische Parameter:	
Host-ID	'A3B3C3D3' (8-stellig, alphanummerisch)
Password	8-stellig, alphanummerisch
Verschlüsselungs-Public-Key des Kunden:	'A1B1C1D1'
Exponent	'00 .. 01 00 00 0F' (Hex)
Lmodulo	'0768'
Modulo	'0 ... a7f885 ... 65' (Hex)
Verwendungszweck ³¹	'05'

Allgemeiner Aufbau des Remote-Filename

Das Feld enthält die inhaltliche Beschreibung des Transferauftrages und gegebenenfalls auftragsspezifische Daten. Nur Byte 1 bis 44 werden genutzt. Die einzelnen Parameter sind durch Punkte voneinander getrennt. Aus Kompatibilitätsgründen beim Empfänger-Betriebssystem ist das erste Byte eines Qualifiers immer ein Alphazeichen. Die Grundstellung für nicht belegte Stellen ist 'N'. Der Aufbau ist:

PV.Kunden-ID.Auftragsart.Auftragsattribut[.Auftragsnummer] [.Auftragsparameter]

Erläuterung:

- PV (2 Bytes alphanummerisch):
Versionsnummer des Anwendungsprotokolls; zur Zeit konstant 'A3'
- Kunden-ID (8 Bytes alphanummerisch):
Bankspezifische Kunden-ID
- Auftragsart-Kennung (3 Bytes alphanummerisch, siehe 1.4 „Auftragsartenkennungen“)

³¹ Das Feld „Verwendungszweck“ ist zunächst ohne Funktion und wird nur vorläufig belegt.

- Auftragsattribut (5 Bytes alphanummerisch):

Byte	Inhalt	Auswahlmöglichkeiten
1	Dateiart	O = Originaldatei mit zugehöriger Unterschriftsdatei U = Unterschriftsdatei D = Originaldatei ohne zugehöriger Unterschriftsdatei B = Originaldatei und EU-Datei in einer physikalischen Datei P = Protokolldatei Y = Dummy-Datei
2	Komprimierungsart ³²	N = Keine Komprimierung F = FLAM-Komprimierung Z = PKZIP-Komprimierung X = x-Press-Komprimierung ... Die zum Einsatz kommenden Komprimierungsprodukte werden durch die ZKA-Buchstabenkennungen festgelegt.
3	Verschlüsselungsart	N = Keine Verschlüsselung H = Hybrid-Verfahren DES/RSA R = RSA
4	Reserve	
5	Reserve	

- Auftragsnummer (4 Bytes alphanummerisch):
Je Kunde eindeutige Auftragsnummer für die Übertragungsrichtung Kunde/Bank. Dient als Ordnungsbegriff bei der PC-Host-Kommunikation, insbesondere beim Protokollabruf und bei der Synchronisation von Original- und Unterschriftsdatei.

Byte	Inhalt
1	A
2	laufende Nummer des Kunden-DFÜ-PCs
3-4	2 Stellen alphanummerisch (werden aufsteigend vergeben)

- Auftragsparameter:
Auftragsspezifische weitere Parameter, falls für die Auftragsart erforderlich bzw. zugelassen. Zur Zeit:

Auftragsart	Auftragsparameter
-------------	-------------------

³² Sofern nichts anderes vereinbart, ist das FLAM-Verfahren das Standard-Komprimierungsverfahren.

Auftragsart	Auftragsparameter
STA	optional Datum-von Datum-bis (VJJMMTT.BJJMMTT)
VPK	Kennung für User-ID des Kunden, der VPK-Auftrag unterschrieben hat Byte 1: U (Kennung für User-ID) Byte 2 – 9: User-ID
alle verschlüsselt zu übertragenden Dateien	Verschlüsselungs-Public-Key-Hashwert (33 Bytes alphanummerisch): Byte 1: H (Kennung für Hashwert) Byte 2-33: Verschlüsselungs-Public-Key in Hex-Darstellung

RSA-Key-Paar-Generierung und Verteilung des Verschlüsselungs-Public-Keys des Kunden zur Verschlüsselung des DEK

Damit der Empfänger verschlüsselter Daten diese wieder entschlüsseln kann, wird der Verschlüsselungsschlüssel zusammen mit der verschlüsselten Originalnachricht übermittelt. Es muss jedoch sichergestellt sein, dass nur der berechtigte Empfänger den Verschlüsselungsschlüssel verwenden kann. Deshalb wird der Verschlüsselungsschlüssel (DEK) seinerseits verschlüsselt. Zu diesem Zweck benötigt der Sender verschlüsselter Daten den öffentlichen RSA-Schlüssel des jeweiligen Empfängers.

Kundenseite Rahmenprogramm:

- Erzeugung und Speicherung von Verschlüsselungs-Public Key (VPK_{Kunde}) und zugehörigem Verschlüsselungs-Secret Key (VSK_{Kunde}).

Im Kundensystem gibt es genau ein RSA-Schlüsselpaar für die Verschlüsselung des Verschlüsselungsschlüssels (DEK). Dies ist im Unterschied zu den RSA-Schlüsselpaaren für die Elektronische Unterschrift zu sehen, bei dem ein Schlüsselpaar pro unterschriftsberechtigtem User eines Kunden generiert wird.

- Generierung der Verschlüsselungs-Public-Key-Datei (VPK_{Kunde})

Die Übertragung der Verschlüsselungs-Public-Key-Datei kann mit einer Elektronischen Unterschrift eines unterschriftsberechtigten Users des Kunden abgesichert werden. In diesem Fall setzt die Übertragung von VPK_{Kunde} die erfolgreiche Ausführung der in Kapitel 2.3.6.1 „PDEK“ beschriebenen Abläufe für mindestens ein für die EU zu verwendendes RSA-Schlüsselpaar voraus. Sollte das Verfahren zur Elektronischen Unterschrift noch nicht initialisiert worden sein, so muss die Generierung des Ini-Briefes erfolgen (siehe auch Kapitel 2.2 „Kryptographische Verfahren des deutschen Kreditgewebes für die Elektronische Unterschrift im Rahmen der Kunde-Bank-Kommunikation“).

Für die Beschreibung der weiteren Abläufe wird auf Kapitel 2.3.6.1 „PDEK“ verwiesen. Die entsprechenden DFÜ-Aufträge erhalten das Auftragsattribut VPK, d. h. die entsprechenden DFÜ-Aufträge sind:

- Beispiel für einen VPK-Auftrag mit Elektronischer Unterschrift:
A3.KUNDE1.VPK.BNNNN.A001.UUSER1
- Beispiel für einen VPK-Auftrag ohne Elektronischer Unterschrift:
A3.KUNDE1.VPK.DNNNN.A001

Bankseite Rahmenprogramm:

Die entsprechenden bankseitigen Abläufe sind in Kapitel 2.3.6.1 „PDEK“ beschrieben. In Ergänzung dazu erfolgen nach der Verifizierung der EU und Eintrag der Prüfungsergebnisse ins EU-Protokoll die folgenden Schritte:

- Erfolgsfall bei EU-Prüfung: Automatische Freischaltung und Speicherung von VPK_{Kunde}
- Fehlerfall bei EU-Prüfung: Ablehnung der Verschlüsselungs-Public-Key-Datei
- Protokollierung der Ergebnisse

Übertragung von verschlüsselten Daten von der Bank zum Kunden

Bankseitige Bereitstellung der Daten:

Unter den im vorherigen Abschnitt beschriebenen Voraussetzungen zur Bereitstellung und Verschlüsselung der Kundendatensätze auf der Bankseite wird hier folgende Funktionalität bereitgestellt:

- Generierung eines zufälligen DES-Schlüssels DEK
- Verschlüsselung der Originalnachricht mit DEK
- Verschlüsselung von DEK mit VPK_{Kunde}
- Konkatenation von Dateivorsatz und verschlüsselter Originalnachricht zu einer V-Datei
- Bereitstellung der V-Datei für den Abholauftrag

Kundenseitiges Empfangen von Daten:

- Einrichten eines DFÜ-Auftrages zum Abholen der V-Datei, z. B. A3.A1B1C1D1.TST.DNHNN
- Empfang der V-Datei
- Entschlüsselung des verschlüsselten DES-Schlüssels aus dem Dateivorsatz mit VSK_{Kunde}
- Entschlüsselung der Nachricht mit dem so erhaltenen DEK

Übertragung von verschlüsselten Daten vom Kunden zur Bank

Die folgende Beschreibung dokumentiert den Ablauf für den Übertragungsweg vom Kunden zur Bank.

Kundenseitige Bereitstellung der Daten:

Unter den im vorherigen Abschnitt beschriebenen Voraussetzungen zur Bereitstellung und

Verschlüsselung der Sendeaufträge auf der Kundenseite wird hier folgende Funktionalität bereitgestellt:

- Generierung eines zufälligen DES-Schlüssels DEK
- Verschlüsselung der Originalnachricht mit DEK
- Verschlüsselung von DEK mit VPB_{Bank}
- Konkatenation von Dateivorsatz und verschlüsselter Originalnachricht zu einer V-Datei
- Bereitstellung der V-Datei für den Sendeauftrag
- Starten der DFÜ ³³

Bankseitiges Empfangen von Daten

- Empfang der V-Datei
- Entschlüsselung des verschlüsselten DES-Schlüssels aus dem Dateivorsatz mit VSB_{Bank}
- Entschlüsselung der Nachricht mit dem so erhaltenen DEK

³³ Sofern eine DFÜ nicht erfolgreich durchgeführt werden konnte, wird die ggf. vorher bereits komprimierte und verschlüsselte Datei für den nächsten Start der DFÜ gespeichert, so dass ein erneuter Komprimierungs- und Verschlüsselungsvorgang nicht mehr erforderlich ist. Das System sollte erkennen, wenn nach einem erfolglosen DFÜ-Auftrag die Originaldatei gelöscht oder verändert wurde, so dass nicht das Komprimat einer früheren Originaldatei zu einer zwischenzeitlich geänderten Originaldatei verschickt wird.

2.3.6.1 PDEK und DES-Schlüssel (DEK)



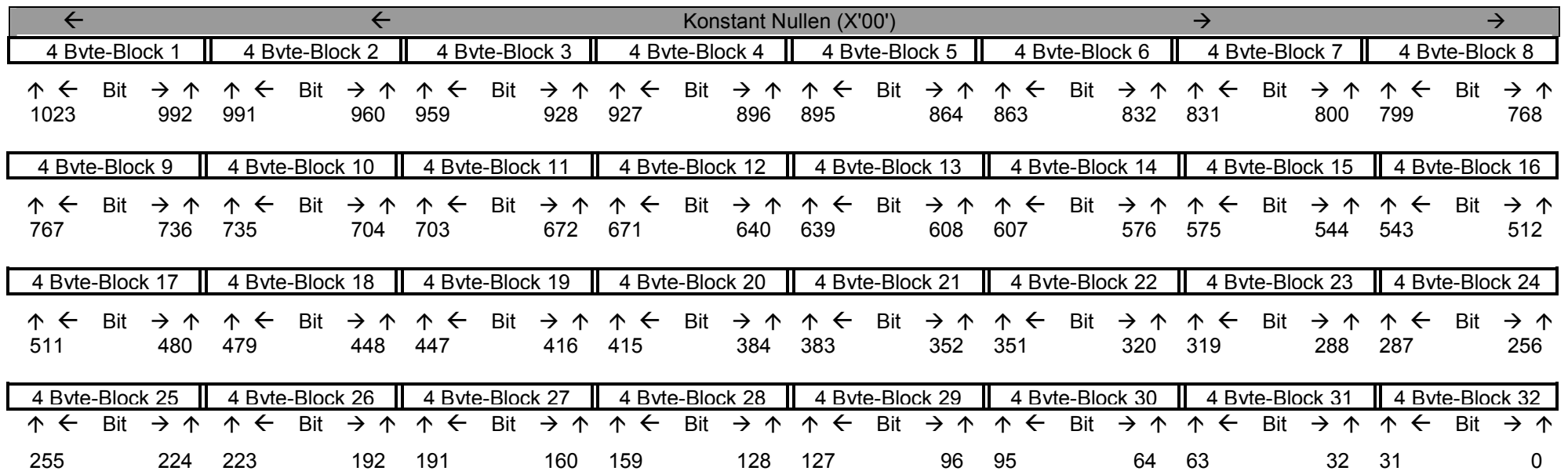
2.3.6.2 EDEK

←				←				Konstant Nullen (X'00')																→				→			
4 Bvte-Block 1				4 Bvte-Block 2				4 Bvte-Block 3				4 Bvte-Block 4				4 Bvte-Block 5				4 Bvte-Block 6				4 Bvte-Block 7				4 Bvte-Block 8			
↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑		
1023			992	991			960	959			928	927			896	895			864	863			832	831			800	799			768
4 Bvte-Block 9				4 Bvte-Block 10				4 Bvte-Block 11				4 Bvte-Block 12				4 Bvte-Block 13				4 Bvte-Block 14				4 Bvte-Block 15				4 Bvte-Block 16			
↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑		
767			736	735			704	703			672	671			640	639			608	607			576	575			544	543			512
4 Bvte-Block 17				4 Bvte-Block 18				4 Bvte-Block 19				4 Bvte-Block 20				4 Bvte-Block 21				4 Bvte-Block 22				4 Bvte-Block 23				4 Bvte-Block 24			
↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑		
511			480	479			448	447			416	415			384	383			352	351			320	319			288	287			256
4 Bvte-Block 25				4 Bvte-Block 26				4 Bvte-Block 27				4 Bvte-Block 28				4 Bvte-Block 29				4 Bvte-Block 30				4 Bvte-Block 31				4 Bvte-Block 32			
↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑	↑	←	Bit	→	↑		
255			224	223			192	191			160	159			128	127			96	95			64	63			32	31			0

The diagram illustrates the structure of a 32-byte data structure, divided into four groups of eight 4-byte blocks each. The first group (blocks 1-8) is labeled 'Konstant Nullen (X'00')' and has arrows pointing left and right. The second group (blocks 9-16) is also labeled 'Konstant Nullen (X'00')' and has arrows pointing left and right. The third group (blocks 17-24) is labeled 'Konstant Nullen (X'00')' and has arrows pointing left and right. The fourth group (blocks 25-32) is labeled 'Konstant Nullen (X'00')' and has arrows pointing left and right. Below the first group, the internal structure of '4 Byte Block 1' and '4 Byte Block 2' is shown. '4 Byte Block 1' contains the hex values 00, 00, 00, 01, and '4 Byte Block 2' contains 00, 00, 00, 0F. Arrows indicate the bit positions for each byte, with the first byte of '4 Byte Block 1' having bits 63, 32, and 0 marked.

Hier wird beispielhaft der Exponent mit dem Wert 00 ... 01 00 00 00 0F (Hex) dargestellt. Gegebenenfalls können auch variable Werte für den Exponenten verwendet werden oder die 4. Fermat'sche Primzahl. Es ist sicherzustellen, dass nicht der schwache Exponent 3 verwendet wird.

2.3.6.4 Modulo



2.3.6.5 Testdaten Verschlüsselung

Testdaten werden nachgereicht

2.3.7 Liste der reservierten Antwortcodes

Antwortcode	Bemerkung
50	Aktion erfolgreich - Neue Bankparameterdaten abholen Das Banksystem hat neue Bankparameterdaten zur Verfügung gestellt. Das Kundensystem generiert automatisch einen BPD-Abholauftrag und informiert den Anwender, dass der Abholauftrag zu starten ist.
51	Verschlüsselungscode mit Bank muss aktualisiert werden. Auf dem Banksystem wurde ein neuer Verschlüsselungs-Public-Key generiert, der vom Kundensystem abgeholt werden muss. Der Anwender wird hierüber durch eine entsprechende Meldung hingewiesen. Solange der neue Verschlüsselungs-Public-Key bei der Bank noch nicht abgeholt wurde, kann der Kunde keine (verschlüsselten) Dateien an die Bank übermitteln. Der Antwortcode 51 kann auch dann vom Banksystem zurückgeliefert werden, wenn der im FTAM-Remote-Filename der verschlüsselten Datei eingestellte Hashwert des verwendeten Verschlüsselungs-Public-Keys der Bank (VPB) nicht mit dem bankseitig erwarteten Hashwert übereinstimmt. In diesem Fall muss der Kunde ebenfalls einen neuen Verschlüsselungs-Public-Key bei der Bank abholen.
52	Daten müssen verschlüsselt abgeholt werden Diese Meldung kann nur auftreten, wenn der Kunde versucht, trotz einer aktivierten bankseitigen Verschlüsselung Daten unverschlüsselt abzuholen.
53	Daten müssen unverschlüsselt abgeholt werden. Diese Meldung kann nur auftreten, wenn der Kunde versucht, Daten verschlüsselt abzuholen, obwohl diese bankseitig unverschlüsselt bereitgestellt werden.
54	Verschlüsselungscode muss neu verschickt werden. Kundenseitig wird nach erfolgreichem Versand des VPK-Auftrages und des dazugehörigen Legitimationsauftrages zunächst davon ausgegangen, dass die entsprechende Authentifizierung bei der Bank mit positivem Ergebnis durchgeführt wurde. Verläuft die bankseitige Unterschriftsprüfung der VPK-Datei jedoch negativ, so erhält das Kundensystem beim Abholversuch von verschlüsselt vereinbarten Auftragsarten den obigen Antwortcode 54.
55	User nicht EU-berechtigt Diese Meldung wird vom Banksystem zurückgegeben, wenn beim Versand einer VPK-Datei mit Elektronischer Unterschrift festgestellt wird, dass der Unterzeichner bei der Bank keine Unterschriftsberechtigung besitzt. Dies kann bereits vor der Übertragung der Datei selbst ermittelt werden, da die User-ID des Unterzeichnenden im FTAM-Remote-Filename übergeben wird.
56	Verschlüsselungscode noch nicht freigegeben. Solange der kundenseitige Verschlüsselungs-Public-Key bankseitig noch nicht authentifiziert wurde, erhält der Kunde bei dem Versuch, Daten mit den Auftragsarten abzuholen, für die die Verschlüsselung mit der Bank vereinbart wurde, den Returncode 56 „Verschlüsselungscode noch nicht freigegeben“.

2.3.8 Abkürzungsverzeichnis

Abkürzung	Bedeutung
CBC	Cipher Block Chaining
DEK	geheimer DES-Schlüssel (Data Encryption Key)
DES	Data Encryption Standard
DFP	Digital Fingerprint
EDEK	verschlüsselter DEK (Encrypted Data Encryption Key)
FP	Fingerprint
HASH	Hashwert
ICV	Initial Chaining Value
n	Modulus eines RSA-Schlüsselsystems
N	Länge von n in Anzahl der Bit
PDEK	Padded Data Encryption Key
SIGNATUR	Signatur einer Nachricht
THASH	um den Zeitstempel ergänzter Hashwert (Time stamped HASH)
TVP	Zeitstempel (Time Variant Parameter)
VPB	Verschlüsselungs-Public-Key-Bank
VPK	Verschlüsselungs-Public-Key-Kunde
VS	Verschlüsselungs-Secret-Key-Bank
VSK	Verschlüsselungs-Secret-Key-Kunde

3 Anlage 3 (Datenformate)

3.1 Inlandszahlungsverkehr

3.1.1 DTAUS0: Zahlungsverkehrssammelauftrag Diskettenformat

Die Datei im Diskettenformat (ASCII Format; ungepackt) hat folgende Dateispezifikation:

Zugelassener Zeichencode ³⁴	Zeichen	Hexcode
Nummerische Zeichen	0 bis 9	X '30' - X '39'
Großbuchstaben	A bis Z	X '41' - X '5A'
<u>Sonderzeichen:</u>		
Leerzeichen	" "	X '20'
Punkt	"."	X '2E'
Komma	","	X '2C'
Kaufmännisches „und“	"&"	X '26'
Trennstrich	"_"	X '2D'
Schrägstrich	"/"	X '2F'
Pluszeichen	"+"	X '2B'
Stern	"*"	X '2A'
Dollar	"\$"	X '24'
Prozentzeichen	"%"	X '25'
Umlaute und ß	"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 bzw. zurückweisen; unzulässige Sonderzeichen kann es in Leerzeichen (Blanks) konvertieren.

Dateiformat:

Direkt-Zugriffsdateien; physische Satzlänge 128 Bytes. Die Datensätze A und E bestehen aus je einem physischen Satz à 128 Bytes.

Die Datensätze C setzen sich aus mindestens 2 Satzabschnitten (physischen Sätzen) à 128 Bytes zusammen.³⁵

Dateiaufbau:

Die logische Datei ist wie folgt aufzubauen:

- Datensatz A = Datenträger-Vorsatz

³⁴ Codierung gemäß DIN 66003 (Ausgabe Juni 1974), Code Tabelle 2, Deutsche Referenz Version.

³⁵ Es darf nur der festgelegte Zeichenvorrat verwendet werden. Insbesondere darf die Datei keine Format-, Trenn- und Steuerzeichen enthalten.

- Datensatz C = Zahlungsaustauschsatz
- Datensatz E = Datenträger-Nachsatz

Eine logische Datei darf nur Gutschriften oder nur Lastschriften enthalten. Abweichungen von dem Aufbau und den Spezifikationen bedürfen besonderer Vereinbarungen.

Bei Verstößen gegen die EDV-spezifischen Konventionen, die zu einem Programmabbruch führen, insbesondere bei falscher Satzlänge und falschem Datenformat, ist der Empfänger berechtigt, die gesamte Datei an den Einreicher zurückzugeben bzw. abzuweisen.

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 Bytes lang.

Feld	Länge in Bytes	Daten-format ³⁶	Inhalt	Erläuterung
1	4	n	Satzlänge	'128'
2	1	an	Satzart	Konstante "A"
3	2	an	Kennzeichen "GK" bzw. "LK", "GB" bzw. "LB"	Hinweis auf Gutschriften (= G) bzw. Lastschriften (= L), Kundendatei (= K), Bankdatei (=B)
4	8	n	Bankleitzahl	Bankleitzahl des Kreditinstituts (Dateiempfänger)
5	8	n	X '30'	nur belegt, wenn Dateiabsender Kreditinstitut ist, sonst Null
6	27	an	Kundenname	Dateiabsender
7	6	n	Datum	Dateierstellungsdatum (TTMMJJ)
8	4	an	X '20'	Leerzeichen (bankinternes Feld)
9	10	n	Kontonummer	Empfänger/Absender Kunde, max. 10 Stellen (rechtsbündig, nicht belegte Stellen Null). Über dieses Konto wird der Gegenwert verrechnet.
10	10	n	Referenznummer des Einreichers	Angabe freigestellt.
11a	15	an	(X '20')	Reserve
11b	8	an	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 Abs. III, Nr. 4 der Sonderbedingungen für Datenfernübertragung genannte Nachweiszeitraum von mindestens vierzehn Kalendertagen erst ab dem genannten Ausführungstermin zu berechnen ist.
11c	24	an	Leerzeichen (X '20')	Reserve
12	1	an	Währungskennzeichen	"1" = Euro
	128			

³⁶ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

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.

Konstanter Teil, 1. Satzabschnitt:

Feld	Länge in Bytes	Datenformat ³⁷	Inhalt	Erläuterung
1	4	n	Satzlänge	logische Satzlänge (konstanter Teil 187 Bytes + Erweiterungsteil(e) zu 29 Bytes), max. '0622' ³⁸)
2	1	an	Satzart	Konstante "C"
3	8	n	Bankleitzahl	erstbeteiligtes Kreditinstitut, freigestellt
4	8	n	Bankleitzahl	Kreditinstitut des Begünstigten/Zahlstelle
5	10	n	Kontonummer	Begünstigter/Zahlungspflichtiger
6	13	n	Wenn nicht benutzt: Nullen	1. Byte = 0, 2.-12. Byte = interne Kundennummer oder Nullen, 13. Byte = 0
7a	2	n	Textschlüssel	Kennzeichnung der Zahlungsart und Textschlüsselergänzungen gemäß Anhang 1
7b	3	n	Textschlüsselergänzung	
8	1	an	X '20'	bankinternes Feld
9	11	n	Null ³⁹	rechtsbündig; Reserve
10	8	n	Bankleitzahl	überweisendes Kreditinstitut/erste Inkassostelle
11	10	n	Kontonummer	Überweisender/Zahlungsempfänger, rechtsbündig
12	11	n	Betrag in Euro einschließlich Nachkommastellen	rechtsbündig
13	3	an	X '20'	Reserve
14a	27	an	Name	Begünstigter/Zahlungspflichtiger, linksbündig
14b	8	an	X '20'	nur zur Abgrenzung des Satzabschnitts (darf keine Daten enthalten)
	128			

³⁷ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

³⁸ Die nur zur Abgrenzung des jeweiligen Satzabschnittes 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.

³⁹ Feld kann bankseitig mit dem DM-Betrag zur Information belegt sein.

Konstanter Teil, 2. Satzabschnitt:

Feld	Länge in Bytes	Daten-format⁴⁰	Inhalt	Erläuterung
15	27	an	Name	Überweisender/Zahlungsempfänger (linksbündig) es sind möglichst kurze Bezeichnungen zu verwenden.
16	27	an	Verwendungszweck	Es sind möglichst kurze Angaben zu machen. Die Angaben haben sich ausschließlich auf den jeweiligen Zahlungsverkehrsvorgang zu beziehen. Am Anfang dieses Feldes sind linksbündig solche Angaben unterzubringen, auf die der Überweisungsempfänger/Zahlungspflichtige möglicherweise maschinell zuzugreifen beabsichtigt oder die der Zahlungsempfänger bei Lastschriften benötigt, falls die Zahlung als unbezahlt bzw. unanbringlich an ihn zurückgeleitet wird. ⁴¹
17a	1	an	Währungskennzeichen	"1" = Euro
17b	2	an	X '20'	Reserve
18	2	n	Erweiterungszeichen	00 = es folgt kein Erweiterungsteil 01-15 = Anzahl der Erweiterungsteile à 29 Bytes

⁴⁰ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

⁴¹ Der Begünstigte/ Zahlungspflichtige kann elektronisch übermittelte Zahlungsinformationen ohne gesonderte Vereinbarung mit dem Überweisenden-/Zahlungsempfänger automatisch weiterverarbeiten, wenn dieser die Angaben im Datenfeld Verwendungszweck C16 wie folgt strukturiert:

Feldkennzeichen	Inhalt
/INV (Invoice)	Rechnungsnummer
/RFB (Reference Beneficiary)	Referenz des Begünstigten
/ROC (Reference Ordering Customer)	Referenz des Überweisenden

Im Zusammenhang mit dem Textschlüssel „54“ (Vermögenswirksame Leistungen) werden bestimmte Verwendungszweckangaben nur durch Textschlüssel-Ergänzungen ausgedrückt. Bei Überweisungen auf Sparkonten von Kreditinstituten erübrigt sich dadurch ein diesbezüglicher Text im Datenfeld C16 Verwendungszweck, das Feld muß insofern leer bleiben. Sofern Sparleistungen jedoch auf Konten von Bausparkassen, Versicherungsunternehmen u. ä. überwiesen werden, ist das Datenfeld „Verwendungszweck“ wie folgt zu belegen:

Bausparkontonummer oder Versicherungsnummer (linksbündig)
Name des Begünstigten

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 "Begünstigter" bzw. "Zahlungspflichtiger" (01)
- bis 13 Erweiterungsteile für "Verwendungszweck" (alle 02) und
- 1 Erweiterungsteil für "Überweisender bzw. Zahlungsempfänger" (03).

Feld	Länge in Bytes	Datenformat ⁴²	Inhalt	Erläuterung
19	2	n	Kennzeichen des Erweiterungsteils	01 = Name des Begünstigten/Zahlungspflichtigen 02 = Verwendungszweck 03 = Name des Überweisenden bzw. des Zahlungsempfängers
20	27	an	Begünstigter bzw. Zahlungspflichtiger/Verwendungszweck/Überweisender 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. Überweisenden im konstanten Teil des Datensatzes C unterzubringen (siehe Erläuterungen zu Feld C 16).
21	2	n	Kennzeichen des Erweiterungsteils	(wie Feld 19)
22	27	an	Daten Erweiterungsteil	(wie Feld 20)
23	11	an	X '20'	nur zur Abgrenzung des Satzabschnitts (keine Berücksichtigung für die Satzlängenangabe im Feld C 1)
	128			

⁴² an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

Variabler Teil, 3. Satzabschnitt:

Feld	Länge in Bytes	Daten-format⁴³	Inhalt	Erläuterung
24	2	n	Kennzeichen des Erweiterungsteils	(wie Feld 19)
25	27	an	Daten des Erweiterungsteils	(wie Feld 20)
26	2	n	Kennzeichen des Erweiterungsteils	(wie Feld 19)
27	27	an	Daten des Erweiterungsteils	(wie Feld 20)
28	2	n	Kennzeichen des Erweiterungsteils	(wie Feld 19)
29	27	an	Daten des Erweiterungsteils	(wie Feld 20)
30	2	n	Kennzeichen des Erweiterungsteils	(wie Feld 19)
31	27	an	Daten des Erweiterungsteils	(wie Feld 20)
32	12	an	X '20'	nur zur Abgrenzung des Satzabschnitts (keine Berücksichtigung für die Satzlängenangabe im Feld C 1)
	128			

Für darüber hinaus noch erforderliche Erweiterungsteile stehen der 4. - 6. Satzabschnitt noch zur Verfügung. Der Aufbau des 4. + 5. Satzabschnitts entspricht dem des 3. Satzabschnitts, Satzabschnitt 6 enthält nur einen Erweiterungsteil.

⁴³ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

Datensatz E (Datei-Nachsatz)

Der Datensatz E dient der Abstimmung; er ist je logische Datei nur einmal vorhanden.

Feld	Länge in Bytes	Daten-format ⁴⁴	Inhalt	Erläuterung
1	4	n	Satzlänge	'0128'
2	1	an	Satzart	Konstante "E"
3	5	an	X '20'	Reserve
4	7	n	Anzahl der Datensätze C	Abstimm-Unterlage
5	13	n	Null	Reserve, rechtsbündig
6	17	n	Summe der Kontonummern (Feld 5 der Datensätze C)	Abstimm-Unterlage
7	17	n	Summe der Bankleitzahlen (Feld 4 der Datensätze C)	Abstimm-Unterlage
8	13	n	Summe der Euro-Beträge (Feld 12 der Datensätze C)	Abstimm-Unterlage
9	51	an	X '20'	nur zur Abgrenzung des Satzabschnitts
	128			

⁴⁴ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

Anhang 1**Erläuterungen zu Feld 7 a und 7 b 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 7 a und 7 b können vorkommen:

Textschlüssel Feld 7a	Textschlüsselergänzung 7b	Erläuterung	Inhalt des Datenfeldes 7
04	000 ⁴⁵	Lastschrift (Abbuchungsauftragsverfahren)	'04000'
05	000 ⁴⁵	Lastschrift (Einzugsermächtigungsverfahren)	'05000'
05	005 ⁴⁶	Lastschrift aus POS-Verfügung - electronic cash	'05005'
05	006 ⁴⁶	Lastschrift aus POS-Verfügung (mit ausländischer Karte) - Maestro	'05006'
05	008 ⁴⁷	Lastschrift aus Kreditkartenumsätzen	'05008'
05	015 ⁴⁶	Lastschrift aus POS-Verfügung - POZ	'05015'
51	000 ⁴⁵	Überweisungs-Gutschrift (z.B. kommerzielle Zahlung)	'51000'
53	000 ⁴⁵	Lohn-, Gehalts-, Renten-Gutschrift	'53000'
54	XXJ ⁴⁸	Vermögenswirksame Leistung (VL)	'54XXJ'
56	000	Überweisungen öffentlicher Kassen	'56000'

⁴⁵ Sofern es sich bei dem Überweisenden/Zahlungsempfänger um einen Gebietsfremden im Sinne der Außenwirtschaftsverordnung handelt, sollte die Textschlüsselergänzung „000“ durch „888“ ersetzt werden.

⁴⁶ Verwendung nur durch Netzbetreiber zugelassen

⁴⁷ Nur für Kreditkartenorganisationen zugelassen

⁴⁸ 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 2001 mit 10%-iger Sparzulage lautet die korrekte Belegung des Datenfeldes 7: „54 001“ oder „54 101“.

Anhang 2**Kontrollmaßnahmen (Plausibilitäts- und Feldinhaltsprüfungen)**

Nach Erhalt und vor Weiterleitung einer Datei im Diskettenformat sind die Datensätze C wie folgt maschinell zu prüfen:

Feld	Inhalt	Datenformat⁴⁹
Bankleitzahl des Kreditinstituts des Begünstigten/der Zahlstelle (Feld C 4)	auf Existenz der Bankleitzahl lt. Bankleitzahlenverzeichnis der Deutschen Bundesbank, 1. Stelle ungleich 0 oder 9	n
Kontonummer des Begünstigten/Zahlungspflichtigen (Feld C 5)	ungleich Null	n
interne Kundennummer (Feld C 6)	1. Byte = Null	n
Textschlüssel Lastschriften Gutschriften (Feld C 7 a)	gleich 04, 05 ⁵⁰ gleich 51, 53, 54, 56 ⁵⁰	n
Bankleitzahl des Kreditinstituts des Überweisenden /der ersten Inkassostelle (Feld C 10)	1. Stelle ungleich 0 oder 9	n
Kontonummer des Überweisenden/Zahlungsempfängers (Feld C 11)	ungleich Null	n
Betrag (Feld C 12)	ungleich Null	n
Name des Begünstigten/Zahlungspflichtigen (Feld C 14)	ungleich X '20'	an
Name des Überweisenden/Zahlungsempfängers (Feld C 15)	ungleich X '20'	an
Währungskennzeichen (Feld C 17a)	"1" = Euro	an
Erweiterungskennzeichen (Feld C 18)	gleich 00-15	n
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	n

Die Kontrollsummen aus der Addition der Stückzahl der Datensätze C, des Feldes „Betrag“ (C12), „Kontonummer des Begünstigten/Zahlungspflichtigen“ (C5) und „Bankleitzahl Kreditinstitut des Begünstigten/Zahlstelle“ (C4) müssen mit den Angaben im Datensatz E übereinstimmen.

⁴⁹ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

⁵⁰ Bei bankseitig ausgelieferten Dateien im Magnetbandformat zusätzlich Textschlüssel 09, 59, 67, bis 69

3.1.2 DTAUS: Zahlungsverkehrssammelauftrag Magnetbandformat

Die Datei im Magnetbandformat (EBCDI-Code, gepacktes Format) hat folgende Dateispezifikation:

Zugelassener Zeichencode ⁵¹	Zeichen	Hexcode
Numerische Zeichen	0 bis 9	
Großbuchstaben	A bis Z	
<u>Sonderzeichen:</u>		
Leerzeichen	" "	X '40'
Punkt	"."	X '4B'
Komma	","	X '6B'
Kaufmännisches „und“	"&"	X '50'
Trennstrich	"-"	X '60'
Schrägstrich	"/"	X '61'
Pluszeichen	"+"	X '4E'
Stern	"*"	X '5C'
Dollar	"\$"	X '5B'
Prozentzeichen	"%"	X '6C'
Umlaute und ß (entweder zweibuchstabig oder siehe rechte Spalte)	"Ä" "Ö" "Ü" "ß"	X '4A' X 'EO' X '5A' X 'A1'

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 bzw. zurückweisen; unzulässige Sonderzeichen kann es in Leerzeichen (Blanks) konvertieren.

Dateiaufbau:

Die logische Datei ist wie folgt aufzubauen:

- Datensatz A = Datenträger-Vorsatz mit 150 Bytes
- Datensatz C = Zahlungsaustauschsatz
konstanter Teil mit 150 Bytes
variabler Teil mit max. 453 Bytes
- Datensatz E = Datenträger-Nachsatz mit 150 Bytes

Eine logische Datei darf nur Gutschriften oder nur Lastschriften enthalten. Abweichungen von dem Aufbau und den Spezifikationen bedürfen besonderer Vereinbarungen.

Bei Verstößen, die zu einem Programmabbruch führen, insbesondere bei falscher Satzlänge und falschem Datenformat, ist der Empfänger berechtigt, die gesamte Datei an den Einreicher zurückzugeben bzw. abzuweisen.

⁵¹ Codierung gemäß DIN 66003 (Ausgabe Juni 1974), Code Tabelle 2, Deutsche Referenz Version.

Datensatz A (Datenträger-Vorsatz)

Der Datensatz A enthält den Dateiabsender und -empfänger; er ist je logische Datei nur einmal vorhanden.

Feld	Länge in Bytes	Daten-format ⁵²	Inhalt	Erläuterung
1	4	b	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlänge. (Satzlängenfeld 4 Bytes, davon 2 Bytes linksbündig binär belegt, restliche Bytes X '40' bzw. X '00').
2	1	an	Satzart	Konstante "A"
3	2	an	Kennzeichen "GK" bzw. "LK", "GB" bzw. "LB"	Hinweis auf Gutschriften (= G) bzw. Lastschriften (= L), Kundendatei (= K), Bankdatei (=B)
4	5	np	Bankleitzahl	Bankleitzahl des Kreditinstituts (Dateiempfänger)
5	5	np	Null	nur belegt, wenn Dateiabsender Kreditinstitut ist, sonst Null (gepackt)
6	27	an	Kundenname	Dateiabsender
7	4	np	Datum	Dateierstellungsdatum ([TTMMJJ], rechtsbündig)
8	4	an	X '40'	Leerzeichen (bankinternes Feld)
9	6	np	Kontonummer	Empfänger/Absender Kunde, max. 10 Stellen (rechtsbündig, nicht belegte Stellen Null). Über dieses Konto wird der Gegenwert verrechnet.
10	10	n	Referenznummer des Einreichers	Angabe freigestellt.
11a	15	an	X '40'	Reserve
11b	8	an	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 Abs. III, Nr. 4 der Sonderbedingungen für Datenfernübertragung genannte Nachweiszeitraum von mindestens vierzehn Kalendertagen erst ab dem genannten Ausführungstermin zu berechnen ist.
11c	58	an	X '40'	Reserve
12	1	an	Währungskennzeichen	"1" = Euro
	150			

⁵² an = alphanummerisch (linksbündig, nicht belegte Stellen X'40'), b = binär, n = numerische Daten ungepackt, np = numerische Daten gepackt, positives Vorzeichen

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.

Konstanter Teil:

Feld	Länge in Bytes	Daten-format ⁵³	Inhalt	Erläuterung
1	4	b	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlänge. (Satzlängenfeld 4 Bytes, davon 2 Bytes linksbündig binär belegt, restliche Bytes X '40' bzw. X '00')
2	1	an	Satzart	Konstante "C"
3	5	np	Bankleitzahl	erstbeteiligtes Kreditinstitut, freigestellt
4	5	np	Bankleitzahl	Kreditinstitut des Begünstigten/Zahlstelle
5	6	np	Kontonummer	Begünstigter/Zahlungspflichtiger, rechtsbündig max. 10 Stellen
6a	6	np ohne Vorzeichen	Interne Kundennummer	1. Halbbyte = 0, 2.-12. Halbbyte = interne Kundennummer oder Nullen
6b	7	np	Nullen	Bankinternes Feld
7a	1	np ohne Vorzeichen	Textschlüssel	Kennzeichnung der Zahlungsart und Textschlüsselergänzungen gemäß Anhang 1
7b	2	np	Textschlüsselergänzung	
8	1	-	X'40'	Bankinternes Feld
9	6	np	Null ⁵⁴	Reserve, rechtsbündig
10	5	np	Bankleitzahl	Kreditinstitut des Überweisenden/erste Inkassostelle
11	6	np	Kontonummer	Überweisender/Zahlungsempfänger, rechtsbündig, max. 10 Stellen
12	6	np	Betrag in Euro einschl. Nachkommastellen	Rechtsbündig
13	3	an	X'40'	Bankinternes Feld
14	27	an	Name	Begünstigter/Zahlungspflichtiger (linksbündig)
15	27	an	Name	Überweisender/Zahlungsempfänger (linksbündig); es sind möglichst kurze Bezeichnungen zu verwenden.

⁵³ an = alphanummerisch (linksbündig, nicht belegte Stellen X'40'), b = binär, n = numerische Daten ungepackt, np = numerische Daten gepackt, positives Vorzeichen

⁵⁴ Feld kann bankseitig mit dem DM-Betrag zur Information belegt sein.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	Daten-format ⁵³	Inhalt	Erläuterung
16	27	an	Verwendungszweck	Es sind möglichst kurze Angaben zu machen. Am Anfang dieses Feldes sind linksbündig solche Angaben unterzubringen, auf die der Begünstigte bei Überweisungen möglicherweise maschinell 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 ⁵⁵ .
17a	1	an	Währungskennzeichen	„1“ = Euro
17b	2	-	X '40'	Reserve
18	2	np	Erweiterungskennzeichen	00 = es folgt kein Erweiterungsteil 01-15 = Anzahl der Erweiterungsteile à 29 Bytes
	150			

⁵⁵ Der Überweisungsempfänger/Zahlungspflichtige kann elektronisch übermittelte Zahlungsinformationen ohne gesonderte Vereinbarung mit dem Überweisenden/Zahlungsempfänger automatisch weiterverarbeiten, wenn dieser die Angaben im Datenfeld „Verwendungszweck“ C16 wie folgt strukturiert:

Feldkennzeichen

Inhalt

/INV (Invoice)

Rechnungsnummer

/RFB (Reference Beneficiary)

Referenz des Begünstigten

/ROC (Reference Ordering Customer)

Referenz des Überweisenden

Im Zusammenhang mit dem Textschlüssel „54“ (Vermögenswirksame Leistungen) werden bestimmte Verwendungszweckangaben nur durch Textschlüssel-Ergänzungen ausgedrückt. Bei Überweisungen auf Sparkonten von Kreditinstituten erübrigt sich dadurch ein diesbezüglicher Text im Datenfeld C16 Verwendungszweck, das Feld muß insofern leer bleiben. Sofern Sparleistungen jedoch auf Konten von Bausparkassen, Versicherungsunternehmen u. ä. überwiesen werden, ist das Datenfeld „Verwendungszweck“ wie folgt zu belegen:

- Bausparkontonummer oder Versicherungsnummer (linksbündig)
- Name des Begünstigten

Variabler Teil:

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 15 Erweiterungsteile unter Beachtung der aufsteigenden Folge des Erweiterungskennzeichens an den konstanten Teil des Datensatzes C angehängt sein. Es können vorkommen:

- 1 Erweiterungsteil für „Begünstigter“ bzw. „Zahlungspflichtiger“ (01)
- bis zu 13 Erweiterungsteile für „Verwendungszweck“ (alle 02) und
- 1 Erweiterungsteil für „Überweisender“ bzw. „Zahlungsempfänger“ (03)

Bei Rücküberweisungen und Rücklastschriften wird der Inhalt von Erweiterungsteilen nicht angegeben. Alle für die Bearbeitung derartiger Rücküberweisungen und Rücklastschriften erforderlichen Verwendungszweckangaben sind daher vom Zahlungsempfänger bzw. Überweisenden im konstanten Teil des Datensatzes C unterzubringen (siehe Erläuterungen zu Feld C 16).

Feld	Länge in Bytes	Datenformat ⁵⁶	Inhalt	Erläuterung
1	2	n	Kennzeichen des Erweiterungsteils	01 = Name des Begünstigten/Zahlungspflichtigen 02 = Verwendungszweck 03 = Name des Überweisenden bzw. des Zahlungsempfängers
2	27	an	Begünstigter bzw. Zahlungspflichtiger/Verwendungszweck/Überweisender bzw. Zahlungsempfänger	Linksbündig. Bei Rücküberweisungen und Rücklastschriften kann der Inhalt von Erweiterungsteilen von den Kreditinstituten nicht angegeben werden. Alle für die Bearbeitung derartiger Rückbelege erforderlichen Verwendungsangaben sind daher vom Zahlungsempfänger bzw. Überweisenden im konstanten Teil des Datensatzes C unterzubringen (siehe Erläuterungen zu Feld C 16).
	29			

⁵⁶ an = alphanummerisch (linksbündig, nicht belegte Stellen X'40'); n = numerische Daten ungepackt.

Datensatz E (Datei-Nachsatz)

Der Datensatz E dient der Abstimmung; er ist je logische Datei nur einmal vorhanden.

Feld	Länge in Bytes	Daten-format⁵⁷	Inhalt	Erläuterung
1	4	b	Satzlänge	Längenangabe des Satzes nach dem Konventionen für variable Satzlänge (Satzlängenfeld 4 Bytes, davon 2 Bytes linksbündig binär belegt, restliche Bytes X'40' bzw. X'00'
2	1	an	Satzart	Konstante "E"
3	5	-	X '40'	Reserve
4	4	n	Anzahl der Datensätze C	Abstimm-Unterlage
5	7	-	Null	Reserve, rechtsbündig
6	9	np	Summe der Kontonummern (Feld 5 der Datensätze C)	Abstimm-Unterlage
7	9	np	Summe der Bankleitzahlen (Feld 4 der Datensätze C)	Abstimm-Unterlage
8	7	np	Summe der Euro-Beträge (Feld 12 der Datensätze C)	Abstimm-Unterlage
9	104	-	X '40'	Reserve
	150			

⁵⁷ an = alphanummerisch (linksbündig, nicht belegte Stellen X'40'); b = binär, n = numerische Daten ungepackt, np = numerische Daten gepackt, positives Vorzeichen

Anhang 1**Erläuterungen zu Feld 7 a und 7 b 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 7 a und 7 b können vorkommen:

Textschlüssel Feld 7a	Textschlüsselergänzung 7b	Erläuterung	Inhalt des Datenfeldes 7
04	000 ⁵⁸	Lastschrift (Abbuchungsauftragsverfahren)	'04000'
05	000 ⁵⁸	Lastschrift (Einzugsermächtigungsverfahren)	'05000'
05	005 ⁵⁹	Lastschrift aus POS-Verfügung - electronic cash	'05005'
05	006 ⁵⁹	Lastschrift aus POS-Verfügung (mit ausländischer Karte) - Maestro	'05006'
05	008 ⁶⁰	Lastschrift aus Kreditkartenumsätzen	'05008'
05	015 ⁵⁹	Lastschrift aus POS-Verfügung - POZ	'05015'
51	000 ⁵⁸	Überweisungs-Gutschrift (z.B. kommerzielle Zahlung)	'51000'
53	000 ⁵⁸	Lohn-, Gehalts-, Renten-Gutschrift	'53000'
54	XXJ ⁶¹	Vermögenswirksame Leistung (VL)	'54XXJ'
56	000	Überweisungen öffentlicher Kassen	'56000'

⁵⁸ Sofern es sich bei dem Überweisenden/Zahlungsempfänger um einen Gebietsfremden im Sinne der Außenwirtschaftsverordnung handelt, sollte die Textschlüsselergänzung „000“ durch „888“ ersetzt werden.

⁵⁹ Verwendung nur durch Netzbetreiber zugelassen.

⁶⁰ Nur für Kreditkartenorganisationen zugelassen.

⁶¹ 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 2001 mit 10%-iger Sparzulage lautet die korrekte Belegung des Datenfeldes 7: „54 001“ oder „54 101“.

Anhang 2**Kontrollmaßnahmen (Plausibilitäts- und Feldinhaltsprüfungen)**

Nach Erhalt und vor Weiterleitung einer Datei im Diskettenformat sind die Datensätze C wie folgt maschinell zu prüfen:

Feld	Inhalt	Datenformat⁶²
Bankleitzahl des Kreditinstituts des Begünstigten/der Zahlstelle (Feld C 4)	auf Existenz der Bankleitzahl lt. Bankleitzahlenverzeichnis der Deutschen Bundesbank, 1. Stelle ungleich 0 oder 9	np
Kontonummer des Begünstigten/Zahlungspflichtigen (Feld C 5)	ungleich Null	np
interne Kundennummer (Feld C 6)	1. Halbbyte = Null ⁶³	np ohne Vorzeichen
Textschlüssel Lastschriften Gutschriften (Feld C 7 a)	gleich 04, 05 ⁶⁴ gleich 51, 53, 54, 56 ⁶⁴	np ohne Vorzeichen
Bankleitzahl des Kreditinstituts des Überweisenden /der ersten Inkassostelle (Feld C 10)	1. Stelle ungleich 0 oder 9	np
Kontonummer des Überweisenden/Zahlungsempfängers (Feld C 11)	ungleich Null	np
Betrag (Feld C 12)	ungleich Null	np
Name des Begünstigten/Zahlungspflichtigen (Feld C 14)	ungleich X '20'	an
Name des Überweisenden/Zahlungsempfängers (Feld C 15)	ungleich X '20'	an
Währungskennzeichen (Feld C 17a)	„1“ = Euro	an
Erweiterungskennzeichen (Feld C 18)	gleich 00-15	np
Kennzeichen des Erweiterungsteils (Feld 1 des variablen Teils im Datensatz C)	gleich 01, 02 oder 03 in aufsteigender Reihenfolge max. 1 mal 01, max. 13 mal 02, max. 1 mal 03	n

Die Kontrollsummen aus der Addition der Stückzahl der Datensätze C, des Feldes „Betrag“ (C12), „Kontonummer des Begünstigten/Zahlungspflichtigen“ (C5) und „Bankleitzahl Kreditinstitut des Begünstigten/Zahlstelle“ (C4) müssen mit den Angaben im Datensatz E übereinstimmen.

⁶² an = alphanummerisch; n = numerische Daten ungepackt, np = numerische Daten gepackt, positives Vorzeichen

⁶³ Bei bankseitig ausgelieferten Dateien im Magnetbandformat erstes Halbbyte gleich „1“ für EZÜ-Zahlungen oder gleich „2“ für BZÜ-Zahlungen

⁶⁴ Bei bankseitig ausgelieferten Dateien im Magnetbandformat zusätzlich Textschlüssel 09, 59, 67 bis 69.

3.1.3 DTAUS: Lastschriftsammelauftrag electronic cash

Die Datei im Diskettenformat (ASCII Format; ungepackt) hat folgende Dateispezifikation:

Zugelassener Zeichencode⁶⁵	Zeichen	Hexcode
Nummerische Zeichen	0 bis 9	X '30' - X '39'
Großbuchstaben	A bis Z	X '41' - X '5A'
<u>Sonderzeichen:</u>		
Leerzeichen	" "	X '20'
Punkt	"."	X '2E'
Komma	","	X '2C'
Kaufmännisches „und“	"&"	X '26'
Trennstrich	"_"	X '2D'
Schrägstrich	"/"	X '2F'
Pluszeichen	"+"	X '2B'
Stern	"*"	X '2A'
Dollar	"\$"	X '24'
Prozentzeichen	"%"	X '25'
Umlaute und ß	"Ä" "Ö" "Ü" "ß"	X '5B' X '5C' X '5D' 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 bzw. zurückweisen; unzulässige Sonderzeichen kann es in Leerzeichen (Blanks) konvertieren.

Dateiformat:

Direkt-Zugriffsdateien; physische Satzlänge 128 Bytes. Die Datensätze A und E bestehen aus je einem physischen Satz à 128 Bytes.

Die Datensätze C setzen sich aus mindestens 2 Satzabschnitten (physischen Sätzen) à 128 Bytes zusammen.⁶⁶

Dateiaufbau:

Die logische Datei ist wie folgt aufzubauen:

- Datensatz A = Datenträger-Vorsatz
- Datensatz C = Zahlungsaustauschsatz
- Datensatz E = Datenträger-Nachsatz

Eine logische Datei darf nur Gutschriften oder nur Lastschriften enthalten. Abweichungen von dem Aufbau und den Spezifikationen bedürfen besonderer Vereinbarungen.

⁶⁵ Codierung gemäß DIN 66003 (Ausgabe Juni 1974), Code Tabelle 2, Deutsche Referenz Version.

⁶⁶ Es darf nur der festgelegte Zeichenvorrat verwendet werden. Insbesondere darf die Datei keine Format-, Trenn- und Steuerzeichen enthalten.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Bei Verstößen gegen die EDV-spezifischen Konventionen, die zu einem Programmabbruch führen, insbesondere bei falscher Satzlänge und falschem Datenformat, ist der Empfänger berechtigt, die gesamte Datei an den Einreicher zurückzugeben bzw. abzuweisen.

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 Bytes lang.

Feld	Länge in Bytes	Daten-format ⁶⁷	Inhalt	Erläuterung
1	4	n	'0128'	Satzlänge
2	1	an	"A"	Satzart (Konstante)
3	2	an	"LK"	Lastschriften (= L), Kundendaten (= K)
4	8	n	Bankleitzahl	Händlerinstitut
5	8	n	X '30'	Null
6	27	an	Kundenname	Absender des Datenträgers
7	6	n	Datum	Erstellungsdatum des Datenträgers (TTMMJJ)
8	4	an	X '20'	Leerzeichen
9	10	n	Kontonummer	Gutschriftskonto, über dieses Konto wird der Gegenwert verrechnet.
10	10	n	Referenznummer des Einreichers	Angabe freigestellt (X'30', falls keine besondere Angabe)
11	47	an	X '20'	Leerzeichen, Reserve
12	1	an	"1" = Euro	Währungskennzeichen
	128			

⁶⁷ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.
Beispiel: 256 = ,0256' = X'30323536' (in 4 Bytes)

Datensatz C (Zahlungsaustauschsatz)**Online-Umsätze****Konstanter Teil, 1. Satzabschnitt:**

Feld	Länge in Bytes	Daten-format⁶⁸	Inhalt	Erläuterung
1	4	n	'0187'	logische Satzlänge (konstanter Teil 187 Bytes)
2	1	an	"C"	Satzart (Konstante)
3	8	n	Null (X'30')	
4	8	n	Bankleitzahl	Bank des Karteninhabers
5	10	n	Kontonummer	Konto des Karteninhabers
6	13	n	Null (X'30')	Bankinternes Feld
7a	2	n	'05'	Textschlüssel: Kennzeichnung Lastschrift
7b	3	n	'005'	Textschlüsselergänzung für nationale ec-Transaktionen
8	1	-	Blank (X '20')	bankinternes Feld
9	11	n	Null (X'30')	rechtsbündig; Reserve
10	8	n	Bankleitzahl	Händlerinstitut (bzw. 1. Inkassostelle)
11	10	n	Kontonummer	Konto des Händlers
12	11	n	Betrag in Euro einschließlich Nachkommastellen	Transaktionsbetrag
13	3	an	Blanks (X '20')	Bankinternes Feld
14a	(27)		ec-interne Angaben	
14a.1	1	an	Transaktionstyp	Siehe ⁶⁹
14a.2	6	n	Trace-Nummer	Vom Terminal vergebene Kennung der Transaktion (BMP 11)
	1	an	Blank	Filler
14a.3	8	an	Autorisierungsmerkmal	Siehe ⁷⁰
	1	an	Blank	Filler

⁶⁸ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

⁶⁹ Mögliche Transaktionstypen: '1' = Online-Autorisierung, feststehender Betrag; '3' = Online-Autorisierung, pauschaler Maximalbetrag

⁷⁰ Das Autorisierungsmerkmal (AID) wird vom AS in die Antwortnachricht eingestellt (Nachrichtentyp 0210 und 0410, BMP 59), wenn der Antwortcode = '00' ist, und stellt dessen elektronischen Stempel dar. Es wird unverändert in den Zahlungsverkehrssatz übernommen.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	Daten-format ⁶⁸	Inhalt	Erläuterung
14a.4	10	an	AID-Parameter	Siehe ⁷¹
14b	8	an	Blanks (X '20')	nur zur Abgrenzung des Satzabschnitts (darf keine Daten enthalten)
	128			

⁷¹ Der AID-Parameter enthält Werte, die zum Berechnen des AID verwendet worden sind. Sein Aufbau ist in Kapitel "Anforderungen an Terminals" beschrieben. Er wird ebenfalls unverändert in den Zahlungsverkehrssatz übernommen.

Konstanter Teil, 2. Satzabschnitt:

Feld	Länge in Bytes	Daten-format ⁷²	Inhalt	Erläuterung
15	27	an	Zahlungsempfänger	Händlerbezeichnung und -ort
16	(27)		Verwendungszweck	
16.1	2 1	an an	"C" Blank	Kennung electronic Cash Filler
16.2	8 1	an an	Terminal-ID Blank	Terminal-Kennung Filler
16.3	5 1	an an	Datum (TT.MM) Blank	Format (Tag.Monat) Filler
16.4	5 1	an an	Uhrzeit (hh.mm) Blank	Format (Stunde.Minute) Filler
16.5	2	an	Kartentyp	Siehe ⁷³
16.6	1	an	Kartenfolgenummer	
17a	1	an	"1"	Währungskennzeichen ("1" = Euro)
17b	2	an	Blanks (X '20')	Reserve
18	2	n	Erweiterungszeichen (00)	00 = es folgt kein Erweiterungsteil
	187			

Variabler Teil (Erweiterungen)

Es ist kein Erweiterungsteil vorgesehen.

⁷² an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

⁷³ Kartentyp:

'ME' - ec-Karte, Magnetstreifen; '

MK' - sonstige Karte, Magnetstreifen (Banken-/Kundenkarte);

'CE' - ec-Karte mit Chip;

'CK' - sonstige Karte mit Chip (Banken- bzw. Kundenkarte).

Offline-Umsätze**Konstanter Teil, 1. Satzabschnitt:**

Feld	Länge in Bytes	Daten-format ⁷⁴	Inhalt	Erläuterung
1	4	n	'0245'	logische Satzlänge (konstanter Teil 187 Bytes + 2 Erweiterungsteile zu 29 Bytes, siehe ⁷⁵)
2	1	an	"C"	Satzart (Konstante)
3	8	n	Null (X'30')	Bankinternes Feld
4	8	n	Bankleitzahl	Bank des Karteninhabers (EF_INFO)
5	10	n	Kontonummer	Konto des Karteninhabers (EF_INFO)
6	13	n	Null (X'30')	Bankinternes Feld
7a	2	n	'05'	Textschlüssel: Kennzeichnung Lastschrift
7b	3	n	'005'	Textschlüsselergänzung für nationale ec-Transaktionen
8	1	an	Blank (X '20')	bankinternes Feld
9	11	n	Null (X'30')	rechtsbündig; Reserve
10	8	n	Bankleitzahl	Händlerinstitut (bzw. 1. Inkassostelle)
11	10	n	Kontonummer	Konto des Händlers
12	11	n	Betrag in Euro (mit Nachkommastellen)	Transaktionsbetrag
13	3	an	Blanks (X '20')	Bankinternes Feld
14a	(27)		ec-interne Angaben	
14a.1	1	an	Transaktionstyp	Siehe ⁷⁶
14a.2	6	n	Sequenznummer	Wert aus EF_SEQ
	1	an	Blank	Filler
14a.3	16	an	Transaktionszertifikat	ZERT aus REDUCE_EC-Kommando
14a.4	10	an	Blanks	Filler
14b	8	an	Blank (X '20')	nur zur Abgrenzung des Satzabschnitts (darf keine Daten enthalten)

⁷⁴ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

⁷⁵ Die Satzlängenangabe bezieht sich nicht auf die physische Satzabschnittlänge der Datei, sondern auf die logische Satzlänge (konstanter Teil 187 Byte + 2 Erweiterungsteile zu je 29 Byte = '0245'). Das nur zur Abgrenzung des Satzabschnittes dienende Feld C23 des variablen Teils 2 des Datensatzes ist in der Satzlängenangabe nicht zu berücksichtigen.

⁷⁶ Mögliche Transaktionstypen: '0' = Offline-Autorisierung, feststehender Betrag; '2' = Offline-Autorisierung, pauschaler Maximalbetrag

Konstanter Teil, 2. Satzabschnitt:

Feld	Länge in Bytes	Daten-format ⁷⁷	Inhalt	Erläuterung
15	27	an	Zahlungsempfänger	Händlerbezeichnung und -ort
16	(27)		Angaben für Tagesauszug	
16.1	2 1	an an	'EC' Blank	Kennung electronic Cash Filler
16.2	8 1	an an	Terminal-ID Blank	Terminal-Kennung Filler
16.3	5 1	an an	Datum (TT.MM) Blank	Format (Tag.Monat) Filler
16.4	5 1	an an	Uhrzeit (hh.mm) Blank	Format (Stunde.Minute) Filler
16.5	2	an	Kartentyp	Siehe ⁷⁸
16.6	1	an	Kartenfolgenummer	Wertniedrigste Ziffer der Kartenfolgenummer aus EF_INFO
17a	1	an	"1"	Währungskennzeichen ("1" = Euro)
17b	2	an	Blanks (X '20')	Reserve
18	2	n	Erweiterungszeichen (02)	Anzahl Erweiterungsteile = 2
	187			

⁷⁷ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

⁷⁸ Kartentyp:

'CE'- ec-Karte mit Chip;

'CK' - sonstige Karte mit Chip (Banken- bzw. Kundenkarte).

Variabler Teil (Erweiterungen)**Erweiterungsteil 1**

Feld	Länge in Bytes	Daten-format⁷⁹	Inhalt	Erläuterung
19	2	n	'02'	Kennzeichnung Erweiterungsteil
20	(27)		ec-interne Angaben	
20.1	2 1	n an	Schlüsselnummer Blank	Aus REDUCE_EC-Kommando, siehe ⁸⁰ Filler
20.2	6 1	an an	Chip-Typ + Kennung Betriebssystem Blank	Byte 22, 23-24 EF_ID, siehe ⁸¹ Filler
20.3.	4 1	n an	Verfalldatum Karte Blank	Byte 11-12 EF_ID Filler
20.4	6 1	n an	Aktivierungsdatum Blank	Byte 13-15 EF_ID Filler
20.5	3 2	an n	Währungsbezeichnung Wertigkeit Währung	Byte 18-20 EF_ID Byte 21 EF_ID
	29			

⁷⁹ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

⁸⁰ Schlüsselnummer aus Antwortdaten REDUCE_EC: Chipkarten Typ 0 - Byte 26, Chipkarten Typ 1 - Byte 29.

⁸¹ Darstellung durch die alpha-nummerisch kodierten Hexadezimalziffern. Für Chipkarten vom Typ 0 sind die Byte 23-24 = '00 00' zu setzen.

Erweiterungsteil 2

Feld	Länge in Bytes	Daten-format ⁸²	Inhalt	Erläuterung
21	2	n	'02'	Kennzeichnung Erweiterungsteil
22	(27)		ec-interne Angaben	
22.1	19 1	n an	Kartenummer Blank	Byte 1-10 aus EF_ID (ohne Feldseparator 'D') Filler
22.2	3	n	Ländercode	Byte 16-17 EF_ID
22.3.	1	n	Prüfziffer Spur 2	Byte 6 EF_INFO
22.4	1	n	Prüfziffer Spur 3	Byte 15 EF_INFO
22.5	2	n	Versionsnummer	Aus REDUCE_EC-Kommando, siehe ⁸³
23	11	an	Blanks	Siehe ⁸⁴
	29			

⁸² an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

⁸³ Versionsnummer aus Antwortdaten REDUCE_EC Chipkarten Typ 0 - Byte 27, Chipkarten Typ 1 - Byte 30.

⁸⁴ Die Satzlängenangabe bezieht sich nicht auf die physische Satzabschnittlänge der Datei, sondern auf die logische Satzlänge (konstanter Teil 187 Byte + 2 Erweiterungsteile zu je 29 Byte = '0245'). Das nur zur Abgrenzung des Satzabschnittes dienende Feld C23 des variablen Teils 2 des Datensatzes ist in der Satzlängenangabe nicht zu berücksichtigen.

Datensatz E (Datei-Nachsatz)

Der Datensatz E dient der Abstimmung; er ist je logische Datei nur einmal vorhanden.

Feld	Länge in Bytes	Daten-format⁸⁵	Inhalt	Erläuterung
1	4	n	'0128'	'0128' Satzlänge
2	1	an	"E"	Satzart (Konstante)
3	5	an	Blanks (X '20')	Reserve
4	7	n	Anzahl der Datensätze C	Abstimm-Unterlage
5	13	n	Null	Reserve, rechtsbündig
6	17	n	Summe der Kontonummern aus Feld C5	Abstimm-Unterlage
7	17	n	Summe der Bankleitzahlen aus Feld C4	Abstimm-Unterlage
8	13	n	Summe der Euro-Beträge aus Feld C12	Abstimm-Unterlage
9	51	an	Blanks (X '20')	nur zur Abgrenzung des Satzabschnitts
	128			

⁸⁵ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

3.1.4 DTAUS: Lastschriftsammelauftrag Maestro

Die Datei im Diskettenformat (ASCII Format; ungepackt) hat folgende Dateispezifikation:

Zugelassener Zeichencode ⁸⁶	Zeichen	Hexcode
Numerische Zeichen	0 bis 9	X '30' - X '39'
Großbuchstaben	A bis Z	X '41' - X '5A'
<u>Sonderzeichen:</u>		
Leerzeichen	" "	X '20'
Punkt	" . "	X '2E'
Komma	" , "	X '2C'
Kaufmännisches „und“	" & "	X '26'
Trennstrich	" - "	X '2D'
Schrägstrich	" / "	X '2F'
Pluszeichen	" + "	X '2B'
Stern	" * "	X '2A'
Dollar	" \$ "	X '24'
Prozentzeichen	" % "	X '25'
Umlaute und ß	" 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 bzw. zurückweisen; unzulässige Sonderzeichen kann es in Leerzeichen (Blanks) konvertieren.

Dateiformat:

Direkt-Zugriffsdateien; physische Satzlänge 128 Bytes. Die Datensätze A und E bestehen aus je einem physischen Satz à 128 Bytes.

Die Datensätze C setzen sich aus mindestens 2 Satzabschnitten (physischen Sätzen) à 128 Bytes zusammen.⁸⁷

Dateiaufbau:

Die logische Datei ist wie folgt aufzubauen:

- Datensatz A = Datenträger-Vorsatz
- Datensatz C = Zahlungsaustauschsatz
- Datensatz E = Datenträger-Nachsatz

⁸⁶ Codierung gemäß DIN 66003 (Ausgabe Juni 1974), Code Tabelle 2, Deutsche Referenz Version.

⁸⁷ Es darf nur der festgelegte Zeichenvorrat verwendet werden. Insbesondere darf die Datei keine Format-, Trenn- und Steuerzeichen enthalten.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Eine logische Datei darf nur Gutschriften oder nur Lastschriften enthalten. Abweichungen von dem Aufbau und den Spezifikationen bedürfen besonderer Vereinbarungen. Bei Verstößen gegen die EDV-spezifischen Konventionen, die zu einem Programmabbruch führen, insbesondere bei falscher Satzlänge und falschem Datenformat, ist der Empfänger berechtigt, die gesamte Datei an den Einreicher zurückzugeben bzw. abzuweisen.

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 Bytes lang.

Feld	Länge in Bytes	Daten-format ⁸⁸	Inhalt	Erläuterung
1	4	n	'0128'	Satzlänge
2	1	an	"A"	Satzart (Konstante)
3	2	an	"LK"	Lastschriften (= L), Kundendaten (= K)
4	8	n	Bankleitzahl	Händlerinstitut
5	8	n	Null (X '30')	
6	27	an	Kundenname	Absender des Datenträgers
7	6	n	Datum	Erstellungsdatum des Datenträgers (TTMMJJ)
8	4	an	Blanks (X '20')	
9	10	n	Kontonummer	Gutschriftskonto - Über dieses Konto wird der Gegenwert verrechnet.
10	10	n	Referenznummer des Einreichers	Angabe freigestellt, X'30' (falls keine besondere Angabe)
11	47	an	Blanks (X '20')	Reserve
12	1	an	"1"	Währungskennzeichen ("1" = Euro)
	128			

⁸⁸ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt. Beispiel: 256 = ,0256' = X'30323536' (in 4 Bytes)

Datensatz C (Zahlungsaustauschsatz) / PC-Format**Online-Umsätze****Konstanter Teil, 1. Satzabschnitt:**

Feld	Länge in Bytes	Daten-format⁸⁹	Inhalt	Erläuterung
1	4	n	'0187'	logische Satzlänge (konstanter Teil 187 Bytes + Erweiterungsteil(e) zu 29 Bytes ⁹⁰)
2	1	an	"C"	Satzart (Konstante)
3	8	n	Bankleitzahl	Erstbeteiligtes Institut (Angabe optional)
4	8	n	Bankleitzahl	Kontoführendes Institut der Übergabestelle
5	10	n	Kontonummer	Konto der Übergabestelle
6a	6	n	Trace-Nummer	Trace-Nummer der Transaktion (aus BMP 11)
6b	7	n	Null	Bankinternes Feld
7a	2	n	'05'	Textschlüssel: Kennzeichnung Lastschrift
7b	3	n	'006'	Textschlüsselergänzung für Maestro-Transaktionen
8	1	an	Blank (X '20')	bankinternes Feld
9	11	n	Null (X'30')	rechtsbündig; Reserve
10	8	n	Bankleitzahl	Kontoführendes Institut des Zahlungsempfängers (bzw. 1. Inkassostelle)
11	10	n	Kontonummer	Konto des Zahlungsempfängers
12	11	n	Betrag in Euro (mit Nachkommastellen)	Transaktionsbetrag (aus BMP 4)
13	3	an	Blanks (X '20')	Bankinternes Feld
14a	(27)		Händler-Info, Teil 1	
14a.1	8	an	Terminal-ID	Terminal-Kennung (aus BMP 41)
14a.2	4	an	Branche	Branchenschlüssel des Händlers (aus BMP 18)
14a.3	15	an	Händlername ⁹¹	Händlername, Teil 1 (aus BMP 43, Byte 1-15)
14b	8	an	Blanks (X '20')	nur zur Abgrenzung des Satzabschnitts (darf keine Daten enthalten)

⁸⁹ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

⁹⁰ Die Satzlangenangabe bezieht sich nicht auf die physische Satzabschnittlänge der Datei, sondern auf die logische Satzlänge (konstanter Teil 187 Bytes + 1 Erweiterungsteil bzw. 8 Erweiterungsteile (bei chipbasierten Transaktionen) zu je 29 Bytes = '0216' bzw. '0419').

⁹¹ Das in BMP 43 vorgesehene Zeichen '>' ('3E') zur Trennung von Händlername und -ort muss vor Übernahme in DTA-Satz in '*' ('2A') umgesetzt werden.

Konstanter Teil, 2. Satzabschnitt:

Feld	Länge in Bytes	Daten-format⁹²	Inhalt	Erläuterung
15	(27)		Händler-Info, Teil 2	
15.1	15	an	Händlername ⁹³	Händlername, Teil 2 (aus BMP 43, Byte 16-30)
15.2	4	an	Blanks	Filler
15.3	7	an	Abwicklungskennzeichen Maestro	Systemkennzeichen für Maestro-Transaktionen (aus BMP 3)
15.4	1	an	Transaktionstyp	siehe ⁹⁴
16	(27)		Verwendungszweck	
16.1	19	an	Primary Account Number (PAN)	Kontodaten (aus BMP 2)
16.2	4	an	Verfalldatum	Verfalldatum der Karte (aus BMP 14)
16.3	1	an	Kartenfolgenummer	Folgenummer der Karte (aus BMP 15)
16.4	3	an	Blanks	Filler
17a	1	an	"1"	Währungskennzeichen ("1" = Euro)
17b	2	an	Blanks (X '20')	Reserve
18	2	n	Erweiterungszeichen	Anzahl der Erweiterungsteile (1 für magnetstreifenbasierte Transaktionen, 8 für chipkartenbasierte Transaktionen)
	187			

⁹² an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

⁹³ Das in BMP 43 vorgesehene Zeichen '>' ('3E') zur Trennung von Händlername und -ort muss vor Übernahme in den DTA-Satz in '*' ('2A') umgesetzt werden.

⁹⁴ Mögliche Transaktionstypen: '1' = Online-Autorisierung, fest stehender Betrag; '3' = Online-Autorisierung, pauschaler Maximalbetrag.

Variabler Teil (Erweiterungen)**Erweiterungsteil 1**

Feld	Länge in Bytes	Daten-format ⁹⁵	Inhalt	Erläuterung
1	2	n	'02'	Kennzeichen Verwendungszweck
2	(27)			Internationale Clearinginformation
2.1	10	an	Händlername ⁹⁶	Händlername, Teil 3 (aus BMP 43, Byte 31-40)
2.2	6	an	Datum (TTMMJJ)	Transaktionsdatum
2.3	4	an	Zeit (hhmm)	Transaktionszeit
2.4	7	an	Autorisierungskennzeichen	Autorisierungskennzeichen des Kartenausgebers (aus BMP 38)

Erweiterungsteil 2

Feld	Länge in Bytes	Daten-format ⁹⁵	Inhalt	Erläuterung
3	2	n	'02'	Kennzeichen Verwendungszweck
4	(27)			Internationale Clearinginformation
4.1	16	an	Anwendungskryptogramm	Transaktionszertifikat der Karte (TC), Tag '9F26'
4.2	2	an	Kryptogramm-information	Tag '9F27'
4.3	8	an		Tag '9F37'
4.4	1	an		Reserve

⁹⁵ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

⁹⁶ Das in BMP 43 vorgesehene Zeichen '>' ('3E') zur Trennung von Händlername und -ort muss vor Übernahme in den DTA-Satz in '*' ('2A') umgesetzt werden.

Erweiterungsteil 3 (nur für chipbasierte Transaktionen)

Feld	Länge in Bytes	Daten-format ⁹⁷	Inhalt	Erläuterung
5	2	n	'02'	Kennzeichen Verwendungszweck
6	(27)			Internationale Clearinginformation
6.1	4	an	Transaktionszähler der Anwendung	Tag '9F36'
6.2	10	an	TVR	Tag '95'
6.3	2	an	Transaktionstyp	Tag '9C'
6.4	4	an	AIP	Tag '82'
6.5	3	an	Länderschlüssel des Terminals	Tag '9F1A'
6.6	4	an	Blanks (X'20')	Reserve

Erweiterungsteil 4 (nur für chipbasierte Transaktionen)

Feld	Länge in Bytes	Daten-format ⁹⁷	Inhalt	Erläuterung
7	2	n	'02'	Kennzeichen Verwendungszweck
8	(27)			Internationale Clearinginformation
8.1	26	an	Anwendungsdatum des Kartenausgebers	Ersten 13 Byte der Anwendungsdaten des Kartenausgebers, Tag '9F10', nicht belegte Stellen mit Blanks auffüllen.
8.2	1	an	Blanks (X'20')	Reserve

Erweiterungsteil 5 (nur für chipbasierte Transaktionen)

Feld	Länge in Bytes	Daten-format ⁹⁷	Inhalt	Erläuterung
9	2	n	'02'	Kennzeichen Verwendungszweck
10	(27)			Internationale Clearinginformation
10.1	26	an	Anwendungsdatum des Kartenausgebers	Byte 14-26 der Anwendungsdaten des Kartenausgebers, Tag '9F10', nicht belegte Stellen mit Blanks auffüllen.
10.2	1	an	Blanks (X'20')	Reserve

⁹⁷ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

Erweiterungsteil 6 (nur für chipbasierte Transaktionen)

Feld	Länge in Bytes	Daten-format ⁹⁸	Inhalt	Erläuterung
11	2	n	'02'	Kennzeichen Verwendungszweck
12	(27)			Internationale Clearinginformation
12.1	12	an	Anwendungsdatum des Kartenausgebers	Byte 27-32 der Anwendungsdaten des Kartenausgebers, Tag '9F10', nicht belegte Stellen mit Blanks auffüllen.
12.2	9	an	Blanks (X'20')	Reserve
12.3	6	an	DF-Name	Byte 1-3 von DF-Name, Tag '84', nicht belegte Stellen mit Blanks auffüllen.

Erweiterungsteil 7 (nur für chipbasierte Transaktionen)

Feld	Länge in Bytes	Daten-format ⁹⁸	Inhalt	Erläuterung
13	2	n	'02'	Kennzeichen Verwendungszweck
14	(27)			Internationale Clearinginformation
14.1	26	an	DF-Name	Byte 4-16 von DF-Name, Tag '84', nicht belegte Stellen mit Blanks auffüllen.
14.2	1	an	Blanks (X'20')	Reserve

Erweiterungsteil 8 (nur für chipbasierte Transaktionen)

Feld	Länge in Bytes	Daten-format ⁹⁸	Inhalt	Erläuterung
15	2	n	'02'	Kennzeichen Verwendungszweck
16	(27)			Internationale Clearinginformation
16.1	6	an	CVM-Resultate	Tag '9F34'
16.2	6	an	Terminalfähigkeiten	Tag '9F33'
16.3	2	an	Terminaltyp	Tag '9F35'
16.4	8	an	IFD-Seriennummer	Tag '9F1E'
16.5	1	an	Kategorisierungscode der Transaktion	Tag '9F53'
16.6	4	an	Versionsnummer der Anwendung des Terminals	Tag '9F09'
	232			

⁹⁸ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

Offline-Umsätze (nur für chipbasierte Transaktionen)**Konstanter Teil, 1. Satzabschnitt:**

Feld	Länge in Bytes	Daten-format ⁹⁹	Inhalt	Erläuterung
1	4	n	'0419'	logische Satzlänge (konstanter Teil 187 Bytes + 8 Erweiterungsteile zu 29 Bytes, siehe ¹⁰⁰)
2	1	an	"C"	Satzart (Konstante)
3	8	n	Bankleitzahl	Erstbeteiligtes Institut (Angabe optional)
4	8	n	Bankleitzahl	Kontoführendes Institut der Übergabestelle
5	10	n	Kontonummer	Konto der Übergabestelle
6a	6	n	Trace-Nummer	Trace-Nummer der Transaktion (Wert des Transaktionszählers, Tag '9F41')
6b	7	n	Null	Bankinternes Feld
7a	2	n	'05'	Textschlüssel: Kennzeichnung Lastschrift
7b	3	n	'006'	Textschlüsselergänzung für Maestro-Transaktionen
8	1	an	Blank (X '20')	bankinternes Feld
9	11	n	Null (X'30')	rechtsbündig; Reserve
10	8	n	Bankleitzahl	Kontoführendes Institut des Zahlungsempfängers (bzw. 1. Inkassostelle)
11	10	n	Kontonummer	Konto des Zahlungsempfängers
12	11	n	Betrag in Euro einschließlich Nachkommastellen	Transaktionsbetrag (aus BMP 4)
13	3	an	Blanks (X '20')	Bankinternes Feld
14a	(27)		Händler-Info, Teil 1	
14a.1	8	an	Terminal-ID	Terminal-Kennung aus BMP 41
14a.2	4	an	Branche	Branchenschlüssel des Händlers aus BMP 18
14a.3	15	an	Händlername ¹⁰¹	
14b	8	an	Blanks	Abgrenzung des Satzabschnitts

⁹⁹ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁰⁰ Die Satzlängenangabe bezieht sich nicht auf die physische Satzabschnittlänge der Datei, sondern auf die logische Satzlänge (konstanter Teil 187 Bytes + 8 Erweiterungsteile (siehe chipbasierte Transaktionen) zu je 29 Bytes = '0419').

¹⁰¹ Das in BMP 43 vorgesehene Zeichen '>' ('3E') zur Trennung von Händlername und -ort muss vor Übernahme in den DTA-Satz in '*' ('2A') umgesetzt werden.

Konstanter Teil, 2. Satzabschnitt:

Feld	Länge in Bytes	Daten-format¹⁰²	Inhalt	Erläuterung
15	(27)		Händler-Info, Teil 2	
15.1	15	an	Händlername ¹⁰³	Händlername, Teil2 (aus BMP 43, Byte 16-30)
15.2	4	an	Blanks (X'20')	Filler
15.3	7	an	Abwicklungskennzeichen Maestro	Systemkennzeichen für Maestro-Transaktionen (aus BMP3)
15.4	1	an	Transaktionstyp	siehe ¹⁰⁴
16	(27)		Verwendungszweck	
16.1	19	an	Primary Account Number (PAN)	
16.2	4	an	Verfalldatum	
16.3	1	an	Kartenfolgenummer	Folgenummer der Karte, Feld 6.3 aus Spur-2-Daten (Tag '57')
16.4	3	an	Blanks	Filler
17a	1	an	„1“	Währungskennzeichen („1“ = Euro)
17b	2	an	Blanks (X'20')	Reserve
18	2	n	Anzahl der Erweiterungsteile (8)	
	187			

¹⁰² an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁰³ Das in BMP 43 vorgesehene Zeichen '>' ('3E') zur Trennung von Händlername und -ort muss vor Übernahme in den DTA-Satz in '*' ('2A') umgesetzt werden.

¹⁰⁴ Mögliche Transaktionstypen: '0' = Offline-Autorisierung, feststehender Betrag; '2' = Offline-Autorisierung, pauschaler Maximalbetrag.

Variabler Teil (Erweiterungen)**Erweiterungsteil 1**

Feld	Länge in Bytes	Daten-format¹⁰⁵	Inhalt	Erläuterung
1	2	n	'02'	Kennzeichen Verwendungszweck
2	(27)			Internationale Clearinginformation
2.1	10	an	Händlername ¹⁰⁶	Händlername, Teil 3 (aus BMP 43, Byte 31-40)
2.2	6	an	Datum (TTMMJJ)	Transaktionsdatum
2.3	4	an	Zeit (hhmm)	Transaktionszeit
2.4	7	an	Blanks (X'20')	Filler

Erweiterungsteile 2-8

Die Erweiterungsteile 2-8 sind vom selben Format wie die Erweiterungsteile 2-8 bei chipbasierten Online-Umsätzen.

¹⁰⁵ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁰⁶ Das in BMP 43 vorgesehene Zeichen '>' ('3E') zur Trennung von Händlername und -ort muss vor Übernahme in den DTA-Satz in '**' ('2A') umgesetzt werden.

Datensatz E (Datei-Nachsatz)

Der Datensatz E dient der Abstimmung; er ist je logische Datei nur einmal vorhanden.

Feld	Länge in Bytes	Daten-format¹⁰⁷	Inhalt	Erläuterung
1	4	n	'0128'	Satzlänge
2	1	an	„E“	Satzart (Konstante)
3	5	an	Blanks (X '20')	Reserve
4	7	n	Anzahl der Datensätze C	Abstimm-Unterlage
5	13	n	Null	Reserve, rechtsbündig
6	17	n	Summe der Kontonummern aus Feld C5	Abstimm-Unterlage
7	17	n	Summe der Bankleitzahlen aus Feld C4	Abstimm-Unterlage
8	13	n	Summe der Euro-Beträge aus Feld C12	Abstimm-Unterlage
9	51	an	Blanks (X '20')	nur zur Abgrenzung des Satzabschnitts
	128			

¹⁰⁷ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

3.1.5 DTAUS: Lastschriftsammelauftrag POZ

Die Datei im Diskettenformat (ASCII Format; ungepackt) hat folgende Dateispezifikation:

Zugelassener Zeichencode¹⁰⁸	Zeichen	Hexcode
Nummerische Zeichen	0 bis 9	X '30' - X '39'
Großbuchstaben	A bis Z	X '41' - X '5A'
<u>Sonderzeichen:</u>		
Leerzeichen	" "	X '20'
Punkt	"."	X '2E'
Komma	","	X '2C'
Kaufmännisches „und“	"&"	X '26'
Trennstrich	"_"	X '2D'
Schrägstrich	"/"	X '2F'
Pluszeichen	"+"	X '2B'
Stern	"*"	X '2A'
Dollar	"\$"	X '24'
Prozentzeichen	"%"	X '25'
Umlaute und ß	"Ä" "Ö" "Ü" "ß"	X '5B' X '5C' X '5D' 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 bzw. zurückweisen; unzulässige Sonderzeichen kann es in Leerzeichen (Blanks) konvertieren.

Dateiformat:

Direkt-Zugriffsdateien; physische Satzlänge 128 Bytes. Die Datensätze A und E bestehen aus je einem physischen Satz à 128 Bytes.

Die Datensätze C setzen sich aus mindestens 2 Satzabschnitten (physischen Sätzen) à 128 Bytes zusammen.¹⁰⁹

Dateiaufbau:

Die logische Datei ist wie folgt aufzubauen:

- Datensatz A = Datenträger-Vorsatz
- Datensatz C = Zahlungsaustauschsatz
- Datensatz E = Datenträger-Nachsatz

Eine logische Datei darf nur Gutschriften oder nur Lastschriften enthalten. Abweichungen von dem Aufbau und den Spezifikationen bedürfen besonderer Vereinbarungen.

¹⁰⁸ Codierung gemäß DIN 66003 (Ausgabe Juni 1974), Code Tabelle 2, Deutsche Referenz Version.

¹⁰⁹ Es darf nur der festgelegte Zeichenvorrat verwendet werden. Insbesondere darf die Datei keine Format-, Trenn- und Steuerzeichen enthalten.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Bei Verstößen gegen die EDV-spezifischen Konventionen, die zu einem Programmabbruch führen, insbesondere bei falscher Satzlänge und falschem Datenformat, ist der Empfänger berechtigt, die gesamte Datei an den Einreicher zurückzugeben bzw. abzuweisen.

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 Bytes lang.

Feld	Länge in Bytes	Daten-format ¹¹⁰	Inhalt	Erläuterung
1	4	n	'0128'	Satzlänge
2	1	an	"A"	Satzart (Konstante)
3	2	an	"LK"	Lastschriften (= L), Kundendaten (= K)
4	8	n	Bankleitzahl	Händlerinstitut
5	8	n	Null (X '30')	
6	27	an	Kundenname	Absender des Datenträgers
7	6	n	Datum	Erstellungsdatum des Datenträgers (TTMMJJ)
8	4	an	Blanks (X '20')	
9	10	n	Kontonummer	Gutschriftskonto - Über dieses Konto wird der Gegenwert verrechnet.
10	10	n	Referenznummer des Einreichers	Angabe freigestellt (X'30', falls keine besondere Angabe)
11	47	an	Blanks (X '20')	Reserve
12	1	an	"1"	Währungskennzeichen ("1" = Euro)
	128			

¹¹⁰ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt. Beispiel:
256 = ,0256' = X'30323536' (in 4 Bytes)

Datensatz C (Zahlungsaustauschsatz)**Konstanter Teil, 1. Satzabschnitt:**

Feld	Länge in Bytes	Daten-format ¹¹¹	Inhalt	Erläuterung
1	4	n	'0187'	logische Satzlänge (konstanter Teil 187 Bytes)
2	1	an	"C"	Satzart (Konstante)
3	8	n	Bankleitzahl	Erstbeteiligtes Institut (Angabe optional)
4	8	n	Bankleitzahl	Kontoführendes Institut der Übergabestelle
5	10	n	Kontonummer	Konto des Karteninhabers
6	13	n	Null (X'30')	Bankinternes Feld
7a	2	n	'05'	Textschlüssel: Kennzeichnung Lastschrift
7b	3	n	'015'	Textschlüsselergänzung ¹¹² für POZ-Transaktionen
8	1	an	Blank (X '20')	bankinternes Feld
9	11	n	Null (X'30')	rechtsbündig; Reserve
10	8	n	Bankleitzahl	Händlerinstitut (bzw. 1. Inkassostelle); Feld C10 muss identisch mit Feld A4 sein
11	10	n	Kontonummer	Händlerkonto; Feld C11 muss identisch mit Feld A9 sein.
12	11	n	Betrag in Euro einschließlich Nachkommastellen	Transaktionsbetrag (aus BMP 4)
13	3	-	Blanks (X '20')	Bankinternes Feld
14a	(27)		POZ-interne Angaben	
14a.1	1	an	Transaktionstyp	Falls Feld C14a.1 = '4', dann POZ <i>mit</i> Sperrenabfrage, Falls Feld C14a.1 = '5', dann POZ <i>ohne</i> Sperrenabfrage
14a.2	6 1	an an	Trace-Nummer Blank	Vom Terminal vergebene Kennung der Transaktion Filler
14a.3	8 1	an an	Referenznummer Blank	Kennzeichen für erfolgte Sperrenabfrage Filler
14a.4	10	an	Referenzparameter	Zusatzinformation für Referenznummer, falls Feld C14a.1 = '4'. Falls Feld C14a.1 = '5', dann ist Feld C14a.4 mit Blanks (X'20') aufzufüllen

¹¹¹ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹¹² Für Zahlungsaustauschsätze aus dem POZ-Verfahren muss neben dem Textschlüssel '05' die Textschlüsselergänzung '015' eingestellt werden. Dies gilt auch für Transaktionen, für die keine Sperrabfrage durchgeführt wurde.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	Daten-format ¹¹¹	Inhalt	Erläuterung
14b	8	an	Blanks (X '20')	nur zur Abgrenzung des Satzabschnitts (darf keine Daten enthalten)

Konstanter Teil, 2. Satzabschnitt:

Feld	Länge in Bytes	Daten-format ¹¹¹	Inhalt	Erläuterung
15	27	an	Zahlungs- empfänger	Händlerbezeichnung und -ort
16	(27)		Verwendungs- zweck	
16.1	3	an	„POZ“	Kennung für POZ
16.2	8	an	Terminal-ID	Terminal-Kennung
	1	an	Blank	Filler
16.3	5	an	Datum(TT.MM)	Format: (Tag.Monat)
	1	an	Blank	Filler
16.4	5	an	Datum(hh.mm)	Format: (Stunde.Minute)
	1	an	Blank	Filler
16.5	2	an	„ME“	Kartentyp
16.6	1	an	Kartenfolge- nummer	
17a	1	an	“1“	Währungskennzeichen ("1" = Euro)
17b	2	an	Blanks (X '20')	Reserve
18	2	n	Erweiterungszei- chen (00)	Es folgt kein Erweiterungsteil
	187			

Erläuterungen zu Feld 14 des Datensatzes C:

Referenznummer: Die Referenznummer wird von der betreffenden Autorisierungszentrale bei der Sperrabfrage vergeben. Die Art der Berechnung ist jeder Autorisierungszentrale freigestellt. Die Referenznummer ermöglicht im Falle von Reklamationen den Nachweis für eine erfolgte Sperrabfrage. Der Konzentrator stellt die vom Autorisierungssystem in der Antwort (0110) übermittelte Referenznummer aus der Bit-Map-Position 59 in den Zahlungsauswechselsatz ein. Wird bei Kaufbeträgen bis zu EUR 30,68 keine Sperrabfrage durchgeführt, ist das Feld mit Leerzeichen zu belegen.

Referenzparameter: Dieser Wert kann bei der Generierung der Referenznummer herangezogen werden. Der Referenzparameter wird wie folgt aufbereitet:

BMP 33

BMP 57

(Kennung AS)

(Verschlüsselungsparameter)

	A ₂	A ₃
--	----------------	----------------	------

LL	LL	LL	GG	VV	Z ₁	...		Z ₁₆
----	----	----	----	----	----------------	-----	--	-----------------

A ₂	A ₃	GG	VV	Z ₁
----------------	----------------	----	----	----------------

Referenzparameter.

BMP	Wert	Bezeichnung
33	A ₂ A ₃	Bytes 2 und 3 der AS-Kennung (Ziffern-Pos. 3 bis 6)
57	GG VV Z ₁	Generation des Masterkey Version des Masterkey Byte 1 der Zufallszahl RND _{MES}

Die angegebenen BMP beziehen sich auf die Antwortnachricht (0110). Der Referenzparameter ist druckaufbereitet (jedes Halbbyte wird in die entsprechenden Zeichen '0', ... , '9', 'A', ... , 'F' umgewandelt) vom Konzentrator in das Feld einzustellen. Wird bei Kaufbeträgen bis zu EUR 30,68 keine Sperrabfrage durchgeführt, ist das Feld mit Leerzeichen zu belegen.

Datensatz E (Datei-Nachsatz)

Der Datensatz E dient der Abstimmung; er ist je logische Datei nur einmal vorhanden.

Feld	Länge in Bytes	Daten-format¹¹³	Inhalt	Erläuterung
1	4	n	'0128'	Satzlänge
2	1	an	"E"	Satzart (Konstante)
3	5	an	Blanks (X '20')	Reserve
4	7	n	Anzahl der Datensätze C	Abstimm-Unterlage
5	13	n	Null (X'30')	Reserve, rechtsbündig
6	17	n	Summe der Kontonummern aus Feld C5	Abstimm-Unterlage
7	17	n	Summe der Bankleitzahlen aus Feld C4	Abstimm-Unterlage
8	13	n	Summe der Euro-Beträge aus Feld C12	Abstimm-Unterlage
9	51	an	Blanks (X '20')	nur zur Abgrenzung des Satzabschnitts
	128			

¹¹³ an = alphanummerisch; n = numerische Daten ungepackt. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

3.2 Auslandszahlungsverkehr

Dieses Kapitel besteht (optisch angepasst an das Layout des hier vorliegenden Dokuments) aus der Anlage 1 (inkl. ihrer 4 Anhänge) des Handbuches „Auslandszahlungsverkehr im Datenaustausch zwischen Kunde und Bank 2003“, Version 2003_2 (Stand 03. Februar 2003) welches ab dem 01. Juli 2003 gültig ist. Die bis zum 30. Juni 2003 gültige Version kann bei Bedarf beim ZKA angefordert werden.

Aufbau und Spezifikation der Datenträger

1. Magnetbandkassetten

Die im beleglosen Datenaustausch zu verwendenden Magnetbandkassetten müssen in ihren technischen Eigenschaften DIN ISO 9661 entsprechen.

(1) Kennsätze: Bandanfang: VOL1 (6-stellig), HDR1, HDR2 (freigestellt), Bandmarke

Bandende: Bandmarke

EOV1 bzw. EOF1, EOVS1 bzw. EOFS1 (freigestellt)

Bandmarke,

Bandmarke (freigestellt)

Zur physischen Band- und Dateikennzeichnung sind Systemkennsätze zu verwenden, die in ihrem Aufbau den Konventionen z.B. der IBM-Systeme 370/30xx/43xx, der Siemens-Systeme 75xx/77xx oder vergleichbarer Systeme entsprechen.

(2) Dateiname: DTAZV (in HDR1 Feld 3). Der Dateiname muss unbedingt am Anfang von Feld 3 des HDR1 stehen. Die Angabe von Zusatzinformationen hinter dem Dateinamen DTAZV ist zugelassen. Diese Zusatzinformationen sind durch einen Punkt (X'4B') von dem Dateinamen DTAZV zu trennen.

Eine Kassette darf nur eine logische Datei mit Zahlungsverkehrsdaten enthalten.

(3) Schreibdichte: 38000 bpi (EBCDI-Code) in 18 Kanalaufzeichnung
oder 76000 bpi (EBCDI-Code) in 36 Kanalaufzeichnung.

(4) Zeichenvorrat (EBCDI-Code):

Zugelassener Zeichencode ¹¹⁴	Zeichen	Hexcode
Nummerische Zeichen	0 bis 9	
Großbuchstaben	A bis Z	
Sonderzeichen:		
Leerzeichen	" "	X '40'
Punkt	" . "	X '4B'
Komma	" , "	X '6B'
Kaufmännisches „und“	" & "	X '50' ¹¹⁵
Trennstrich	" - "	X '60'
Schrägstrich	" / "	X '61'
Pluszeichen	" + "	X '4E'
Stern	" * "	X '5C' ¹¹⁵
Dollar	" \$ "	X '5B' ¹¹⁵
Prozentzeichen	" % "	X '6C' ¹¹⁵

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.

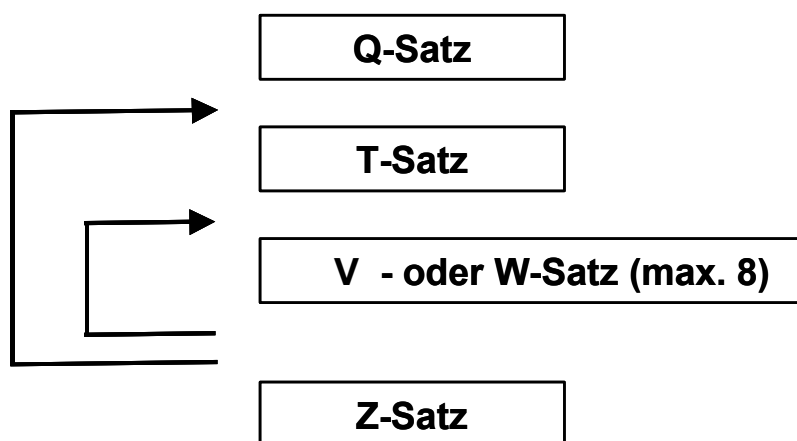
(5) Dateiaufbau: Die Datei enthält Sätze der folgenden Satzarten:

- Q Daten-Vorsatz mit 256 Bytes
- T Einzelzahlungssatz mit 768 Bytes
- V Meldedatensatz zum Transithandel mit 256 Bytes
- W Meldedatensatz für Dienstleistungs-, Kapitalverkehr und Sonstiges mit 256 Bytes
- Z Daten-Nachsatz mit 256 Bytes

Die Datensätze Q und Z gibt es nur einmal. Die restlichen Datensätze können mehrmals vorkommen, ihre Reihenfolge ist lediglich durch ihren logischen Zusammenhang bestimmt und wird in der folgenden Abbildung schematisch dargestellt.

¹¹⁴ Codierung gemäß DIN 66003 (Ausgabe Juni 1974), Code Tabelle 2, Deutsche Referenz Version.

¹¹⁵ Z.Zt. nicht zugelassen.



(6) Magnetbandkassettenaufbau: Nach den Konventionen für variable Satzlänge.

(7) Dateikontrollblock: Satzformat: variabel geblockt (VB)
 Satzlänge: 768 Bytes incl. Satzlängenfeld
 Blocklänge: max. 32000 Bytes incl. Blocklängenfeld

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 das Kreditinstitut berechtigt, die gesamte Kassette unbearbeitet zurückzugeben.

2. 3 ½ - Zoll-Disketten

Für die im beleglosen Datenaustausch zu verwendenden 3 ½-Zoll-Disketten gelten bezüglich der Dateiorganisation die Konventionen der MS-DOS¹¹⁶ Betriebssysteme ab Version 3.0. Unterverzeichnisse sind nicht zulässig.

Die Aufzeichnung muss in doppelter Zeichendichte erfolgen. Die Disketten können ein- oder zweiseitig beschrieben werden. Es sind nur solche Disketten zulässig, die vom Hersteller als für die Aufzeichnungsdichten „DD“ (Double Density) bzw. „HD“ (High Density) und zweiseitige Beschriftung (DS) geeignet ausgewiesen sind. Weiterhin gelten folgende Spezifikationen:

¹¹⁶ MS-DOS ist ein Warenzeichen der Microsoft Corp

- (1) Aufzeichnung:
- 80 Spuren (48 tpi)
 - 9 Sektoren je Spur (bei Double Density/ „DD“)
 - 18 Sektoren je Spur (bei High Density/ „HD“)
 - 512 Bytes je Sektor

- (2) Dateiname: **DTAZV** (Dateinamen-Ergänzung nicht belegt).

Eine Diskette darf nur eine logische Datei mit Zahlungsverkehrsdaten enthalten.

- (3) Zeichencode:

Die Datei im Diskettenformat (ASCII Format; ungepackt) hat folgende Dateispezifikation:

Zugelassener Zeichencode ¹¹⁷	Zeichen	Hexcode
Nummerische Zeichen	0 bis 9	X '30' - X '39'
Großbuchstaben	A bis Z	X '41' - X '5A'
<u>Sonderzeichen:</u>		
Leerzeichen	" "	X '20'
Punkt	"."	X '2E'
Komma	","	X '2C'
Kaufmännisches „und“	"&"	X '26' ¹¹⁸
Trennstrich	"_"	X '2D'
Schrägstrich	"/"	X '2F'
Pluszeichen	"+"	X '2B'
Stern	"*"	X '2A' ¹¹⁸
Dollar	"\$"	X '24' ¹¹⁸
Prozentzeichen	"%"	X '25' ¹¹⁸
Umlaute und ß	"Ä" "Ö" "Ü" "ß"	X '5B' X '5C' X '5D' X '7E'

Für den richtigen Ausdruck davon abweichender Zeichen übernehmen die Kreditinstitute keine Haftung.

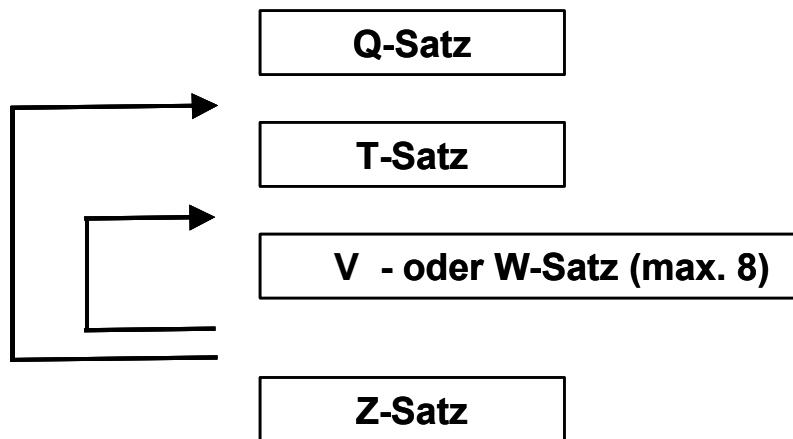
¹¹⁷ Codierung gemäß DIN 66003 (Ausgabe Juni 1974), Code Tabelle 2, Deutsche Referenz Version.

¹¹⁸ Z.Zt. nicht zugelassen

(5) Dateiaufbau: Die Datei enthält Sätze der folgenden Satzarten:

- Q Daten-Vorsatz mit 256 Bytes
- T Einzelzahlungssatz mit 768 Bytes
- V Meldedatensatz zum Transithandel mit 256 Bytes
- W Meldedatensatz für Dienstleistungs-, Kapitalverkehr und Sonstiges mit 256 Bytes
- Z Daten-Nachsatz mit 256 Bytes

Die Datensätze Q und Z gibt es nur einmal. Die restlichen Datensätze können mehrmals vorkommen, ihre Reihenfolge ist lediglich durch ihren logischen Zusammenhang bestimmt und wird in der folgenden Abbildung schematisch dargestellt.



Mehrdiskettendateien (= eine Datei auf mehreren Disketten) sind nicht zulässig.

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 das Kreditinstitut berechtigt, die gesamte Diskette unbearbeitet zurückzugeben

Aufbau der Datensätze**Datensatz Q (Datei-Vorsatz)**

Dieser Satz enthält kundenbezogene Informationen, die in der gesamten Datei Gültigkeit haben. Der Vorsatz ist nur einmal pro logischer Datei enthalten.

Feld	Länge in Bytes	1. Stelle im Satz	Feld art ¹¹⁹	Daten- format¹²⁰	Inhalt	Erläuterungen
1	4	1	P	binär/ num	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlänge (binär bei Magnetbandkassetten, numerisch bei Disketten)
2	1	5	P	alpha	Satzart	Konstante "Q"
3	8	6	P	num	BLZ	Dateiempfangendes Kreditinstitut
4	10	14	P	num	Kundennummer	Ordnungsnummer gemäß Vereinbarung mit dem dateiempfangenden Kreditinstitut (ggf. Kontonummer)
5	4x35	24	P	alpha	Auftraggeberdaten	Zeile 1 und 2: Name Zeile 3 :Straße / Postfach Zeile 4 :Ort
6	6	164	P	num	Erstellungsdatum	Format: JJMMTT
7	2	170	P	num	laufende Nummer	Laufende Tagesnummer
8	6	172	P	num	(erster) Ausführ- ungstermin Datei	Format: JJMMTT; gleich oder bis zu höchstens 15 Kalendertage nach dem Datum aus Feld Q6

¹¹⁹ K = Kannfeld, P = Pflichtfeld, K/P = Pflichtfeld in Abhängigkeit von bestimmten Kriterien, N = nicht belegbares Feld

¹²⁰ alpha = alphanummerische Daten (linksbündig, nicht belegte Stellen: Leerzeichen), num = numerische Daten (rechtsbündig, nicht belegte Stellen: Nullen)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Feld art 119	Daten- format ¹²⁰	Inhalt	Erläuterungen
9	1	178	P	alpha	Weiterleitung an die Meldebehörde	Soll das dateiempfangende Kreditinstitut Meldedaten zu den nachfolgenden Zahlungen an die Bundesbank weiterleiten ? (<i>siehe Erläuterungen im Anhang 3</i>) 'J' Ja 'N' Nein
10	2	179	K/P	num	Bundeslandschlüssel	Zwingend belegt, wenn Meldedaten zu den Zahlungen an die Bundesbank weitergeleitet werden sollen. ('J' in Feld Q9)
11	8	181	K/P	num	Firmennummer / BLZ des Auftraggebers	Siehe Erläuterungen Feld Q10
12	68	189	N	alpha		Reserve
	256					

Datensatz T (Einzelzahlungssatz)

Der Einzeldatensatz enthält Informationen über den auszuführenden Transferauftrag.

Feld	Länge in Bytes	1. Stelle im Satz	Daten-format ¹²¹	Inhalt	Erläuterungen allgemein	Feldart ¹²² allgemeine Zahlungen ¹²³	EU-Standardüberweisungen ¹²⁴		EUE-Überweisungen ¹²⁵	
							Feld-art ¹²²	Besondere Belegungsvorschriften	Feld-art ¹²²	Besondere Belegungsvorschriften
1	4	1	binär / num	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlänge (binär bei Magnetbandkassetten, numerisch bei Disketten)	P	P		P	
2	1	5	alpha	Satzart	Konstante "T"	P	P		P	
3	8	6	num	BLZ	BLZ der kontoführenden Stelle des mit dem Auftragswert zu belastenden Kontos (Feld T4b)	P	P		P	

¹²¹ alpha = alphanummerische Daten (linksbündig, nicht belegte Stellen: Leerzeichen), num = numerische Daten (rechtsbündig, nicht belegte Stellen: Nullen)

¹²² K = Kannfeld, P = Pflichtfeld, K/P = Pflichtfeld in Abhängigkeit von bestimmten Kriterien, N = nicht belegbares Feld

¹²³ d.h. alle Zahlungen außer EU-Standardüberweisungen und EUE-Überweisungen

¹²⁴ Eine „EU-Standardüberweisung“ ist eine grenzüberschreitende Überweisung gemäß Artikel 2 a) i) der Verordnung Nr. 2560/2001 des Europäischen Parlaments und des Rates der Europäischen Union über grenzüberschreitende Überweisungen in Euro, die in Euro bis zu einem Betrag von 12.500 Euro lautet und bei der laut Artikel 5 (2) die IBAN des Begünstigten und der BIC des Kreditinstitutes des Begünstigten anzugeben sind.

¹²⁵ Taggleiche Eilüberweisung in Euro. Bitte beachten Sie die institutsindividuellen Cut-Off-Zeiten für EUE-Zahlungen.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Daten-format ¹²¹	Inhalt	Erläuterungen allgemein	Feldart ¹²² allgemeine Zahlungen ¹²³	EU-Standardüberweisungen ¹²⁴		EUE- Überweisungen ¹²⁵	
							Feld-art ¹²²	Besondere Belegungsvorschriften	Feld-art ¹²²	Besondere Belegungsvorschriften
4a	3	14	alpha	ISO-Währungscode	Für mit Auftragswert zu belastendes Konto.	P	P	Nur 'EUR' zulässig	P	Nur 'EUR' zulässig
4b	10	17	num	Kontonummer	Mit Auftragswert zu belastendes Konto	P	P		P	
5	6	27	num	Ausführungstermin Einzelzahlung, wenn abweichend von Feld Q8	Format: JJMMTT; gleich oder nach dem Datum aus Feld Q8, jedoch bis zu höchstens 15 Kalendertage nach dem Datum aus Feld Q6; fehlt der Termin in T5, so wird das Datum in Q8 als Ausführungstermin angenommen.	K	K		K	
6	8	33	num	BLZ	BLZ der kontoführenden Stelle des mit Entgelten und Auslagen zu belastenden Kontos (belegt, wenn dieses Konto abweicht von Auftragswertkonto)	K/P	N		K/P	
7a	3	41	alpha	ISO-Währungscode	Währungscode des mit Entgelten und Auslagen zu belastenden Kontos. (belegt, wenn dieses Konto abweicht von Auftragswertkonto)	K/P	N		K/P	Nur 'EUR' zulässig

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Daten-format ¹²¹	Inhalt	Erläuterungen allgemein	Feldart ¹²² allgemeine Zahlungen ¹²³	EU-Standardüberweisungen ¹²⁴		EUE- Überweisungen ¹²⁵	
							Feld-art ¹²²	Besondere Belegungsvorschriften	Feld-art ¹²²	Besondere Belegungsvorschriften
7b	10	44	num	Kontonummer	Kontonummer des mit Entgelten und Auslagen zu belastenden Kontos. (belegt, wenn dieses Konto abweicht von Auftragswertkonto)	K/P	N		K/P	
8	11	54	alpha	Bank Identifier Code (BIC) der Bank des Begünstigten oder sonstige Identifikation, z.B. CHIPS-ID	Sofern die Zahlung an ein deutsches Kreditinstitut erfolgt, alternativ auch die BLZ des Begünstigten, wobei dieser drei Schrägstriche voranzustellen sind. (Nicht zu belegen bei Scheckziehungen, d.h. bei den Zahlungsartschlüsseln 20-23 und 30-33 in Feld T22)	K/P	P	Bank Identifier Code (BIC) ist Pflicht. Institut muss in einem der Länder gemäß Anhang 4 ansässig sein.	P	Bank Identifier Code (BIC) ist Pflicht.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Daten-format ¹²¹	Inhalt	Erläuterungen allgemein	Feldart ¹²² allgemeine Zahlungen ¹²³	EU-Standardüberweisungen ¹²⁴		EUE- Überweisungen ¹²⁵	
							Feld-art ¹²²	Besondere Belegungsvorschriften	Feld-art ¹²²	Besondere Belegungsvorschriften
9a	3	65	alpha	Ländercode für Bank des Begünstigten	2-stelliger ISO-alpha-Ländercode gemäß Länderverzeichnis für die Zahlungsbilanzstatistik; linksbündig zu belegen; 3. Stelle Leerzeichen (Pflichtfeld, wenn Feld T8 nicht belegt; nicht zu belegen bei Scheckziehungen, d.h. bei den Zahlungsartschlüsseln 20-23 und 30-33 in Feld T22)	K/P	N		N	
9b	4X35	68	alpha	Anschrift der Bank des Begünstigten	Pflichtfeld, wenn Feld T8 nicht mit BIC-Adresse bzw. - bei Zahlungen an ein deutsches Kreditinstitut - nicht mit BLZ belegt; sofern Anschrift nicht bekannt, Konstante „UNBEKANNT“ Zeile 1 und 2: Name Zeile 3 : Straße Zeile 4 : Ort (Nicht zu belegen bei Scheckziehungen, d.h. bei den Zahlungsartschlüsseln 20-23 und 30-33 in Feld T22)	K/P	N		N	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Daten-format ¹²¹	Inhalt	Erläuterungen allgemein	Feldart ¹²² allgemeine Zahlungen ¹²³	EU-Standardüberweisungen ¹²⁴		EUE- Überweisungen ¹²⁵	
							Feld-art ¹²²	Besondere Belegungsvorschriften	Feld-art ¹²²	Besondere Belegungsvorschriften
10a	3	208	alpha	Ländercode für Land des Begünstigten bzw. Scheckempfängers	2-stelliger ISO-alpha-Ländercode gemäß Länderverzeichnis für die Zahlungsbilanzstatistik; linksbündig zu belegen; 3. Stelle Leerzeichen	P	P		P	
10b	4X35	211	alpha	Begünstigter bzw. Scheckempfänger	Bei Zahlungsauftrag: Begünstigter Bei Scheckziehung: Scheckempfänger Zeile 1 und 2: Name Zeile 3 : Straße Zeile 4 : Ort/Land.	P	P	Angabe eines Scheckempfängers nicht möglich	P	Angabe eines Scheckempfängers nicht möglich
11	2X35	351	alpha	Ordervermerk	Nur belegt bei Scheckziehung (d.h. bei den Zahlungsartschlüsseln 20-23 und 30-33 in Feld T22) und Abweichung vom Inhalt der Zeilen 1 und 2 des Feldes T10b	K/P	N		N	
12	35	421	alpha	IBAN bzw. Kontonummer des Begünstigten	IBAN oder Begünstigtenkonto, linksbündig, mit Schrägstrich beginnend. (Nicht zu belegen bei Scheckziehungen, d.h. bei den Zahlungsartschlüsseln 20-23 und 30-33 in Feld T22)	K/P	P	Nur IBAN zulässig; Linksbündig, mit Schrägstrich beginnend.	P	Nur IBAN zulässig; Linksbündig, mit Schrägstrich beginnend.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Daten-format ¹²¹	Inhalt	Erläuterungen allgemein	Feldart ¹²² allgemeine Zahlungen ¹²³	EU-Standardüberweisungen ¹²⁴		EUE- Überweisungen ¹²⁵	
							Feld-art ¹²²	Besondere Belegungs-vorschriften	Feld-art ¹²²	Besondere Belegungs-vorschriften
13	3	456	alpha	Auftragswäh-rung	ISO-Code der zu zahlenden Währung	P	P	Nur ‚EUR‘ zulässig	P	Nur ‚EUR‘ zulässig
14a	14	459	num	Betrag (Vorkomma-stellen)	Rechtsbündig	P	P	Nur Beträge bis maximal 12.500 EUR zulässig	P	
14b	3	473	num	Betrag (Nachkom-mastellen)	Linksbündig	P	P		P	
15	4X35	476	alpha	Verwen-dungszweck		K	K		K	
16	2	616	num	Weisungs-schlüssel 1 (gem. Anhang 2)	Nicht zu belegen bei Scheckziehungen, (d.h. bei den Zahlungsartschlüsseln 20-23 und 30-33 in Feld T22)	K	N		K	Nur Wei-sungsschlüs-sel ‚10‘, ‚11‘ und ‚12‘ aus Anhang 2 zulässig

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Daten-format ¹²¹	Inhalt	Erläuterungen allgemein	Feldart ¹²² allgemeine Zahlungen ¹²³	EU-Standardüberweisungen ¹²⁴		EUE- Überweisungen ¹²⁵	
							Feld-art ¹²²	Besondere Belegungsvorschriften	Feld-art ¹²²	Besondere Belegungsvorschriften
17	2	618	num	Weisungsschlüssel 2 (gem. Anhang 2)	Nicht zu belegen bei Scheckziehungen, (d.h. bei den Zahlungsartschlüsseln 20-23 und 30-33 in Feld T22)	K	N		K	Nur Weisungsschlüssel ,10', ,11' und ,12' aus Anhang 2 zulässig
18	2	620	num	Weisungsschlüssel 3 (gem. Anhang 2)	Mit ,95' zu belegen, falls Meldedatensätze V bzw. W folgen und falls die Zahlung keine Euro-Gegenwertzahlung ist (vgl. Feld T19). ¹²⁶ Bei Scheckziehungen , d.h. bei den Zahlungsartschlüsseln 20-23 und 30-33 in Feld T22 nur '95' möglich.	K	N		K	Nur Weisungsschlüssel ,10', ,11' und ,12' aus Anhang 2 zulässig

¹²⁶ Die Kennzeichnung ,95' entfällt ab 1.1.2005.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Daten-format ¹²¹	Inhalt	Erläuterungen allgemein	Feldart ¹²² allgemeine Zahlungen ¹²³	EU-Standardüberweisungen ¹²⁴		EUE- Überweisungen ¹²⁵	
							Feld-art ¹²²	Besondere Belegungsvorschriften	Feld-art ¹²²	Besondere Belegungsvorschriften
19	2	622	num	Weisungsschlüssel 4 (gem. Anhang 2 und 2a)	Mit '91' zu belegen im Falle von "Euro-Gegenwertzahlungen" (<i>vgl. Anhang 2a</i>) Bei Scheckziehungen, d.h. bei den Zahlungsartschlüsseln 20-23 und 30-33 in Feld T22 nur '91' möglich.	K/P	N		K	Nur Weisungsschlüssel ,10', ,11' und ,12' aus Anhang 2 zulässig
20	25	624	alpha	Zusatzinformationen zum Weisungsschlüssel	Z. B. Telex, Tel.-Nr., Kabelanschrift (Nicht zu belegen bei Scheckziehungen, d.h. bei den Zahlungsartschlüsseln 20-23 und 30-33 in Feld T22)	K	N		K	Nur bei Weisungsschlüssel ,10' aus Anhang 2 zulässig

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Daten-format ¹²¹	Inhalt	Erläuterungen allgemein	Feldart ¹²² allgemeine Zahlungen ¹²³	EU-Standardüberweisungen ¹²⁴		EUE- Überweisungen ¹²⁵	
							Feld-art ¹²²	Besondere Belegungsvorschriften	Feld-art ¹²²	Besondere Belegungsvorschriften
21	2	649	num	Entgeltregelung	00 = Entgelte zu Lasten Auftraggeber / fremde Entgelte und Auslagen zu Lasten Begünstigter 01 = alle Entgelte und Auslagen zu Lasten Auftraggeber 02 = alle Entgelte und Auslagen zu Lasten Begünstigter (Bei Scheckziehung, d.h. bei Zahlungsartschlüssel 20-23 und 30-33 in Feld T22 nur ,00' möglich)	K/P	P	Nur '00' zugelassen	K/P	
22	2	651	num	Kennzeichnung der Zahlungsart	Gemäß Anhang 1; Zahlungen, die weder '11' noch '13' als Zahlungsartschlüssel enthalten, gelten als allgemeine Zahlungen.	P	P	Nur Zahlungsartschlüssel ,13' aus Anhang 1 zulässig	P	Nur Zahlungsartschlüssel ,11' aus Anhang 1 zulässig
23	27	653	alpha	Variabler Text nur für Auftraggeberabrechnung	Vom Auftraggeber frei belegbar (z.B. Referenz-Nr.); wird nicht weitergeleitet; weiterzuleitende Informationen in Feld T15 angeben. (nur nach Absprache mit dem Kreditinstitut)	K	K		K	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Daten-format ¹²¹	Inhalt	Erläuterungen allgemein	Feldart ¹²² allgemeine Zahlungen ¹²³	EU-Standardüberweisungen ¹²⁴		EUE- Überweisungen ¹²⁵	
							Feld-art ¹²²	Besondere Belegungs-vorschriften	Feld-art ¹²²	Besondere Belegungs-vorschriften
24	35	680	alpha	Name und Telefon-nummer so-wie ggf. Stellvertre-tungs-meldung	Ansprechpartner beim Auf-traggeber für eventuelle Rückfragen der beauftrag-ten Bank oder der Melde-behörde. Dahinter, wenn Auftraggeber nicht Zah-lungspflichtiger ist: 'INV' ohne Leerstellen gefolgt von: Bundesland-Nummer (2-stellig) und: Firmennummer bzw. BLZ (8-stellig) des Zahlungspflichtigen	K/P	K	Ansprech-partner beim Auftragge-ber für even-tuelle Rück-fragen der beauftragten Bank	K/P	
25	1	715	num	Meldeschlüs-sel	Nur belegt, wenn die Wei-terleitung des Zahlungsauf-trages an die Bundesbank auf die statistischen An-gaben beschränkt werden soll; (dies sind die Datensätze V, W und Q (ohne Feld Q4) und die Felder 3, 5, 8, 9a, 9b, 10a, 10b, 13, 14a, 14b, 15, 16, 17, 18, 19 und 24 - 27 des Datensatzes T). Belegung in diesem Falle : '1'	K	N		K	
26	51	716	alpha		Reserve	N	N		N	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Daten-format ¹²¹	Inhalt	Erläuterungen allgemein	Feldart ¹²² allgemeine Zahlungen ¹²³	EU-Standardüberweisungen ¹²⁴		EUE- Überweisungen ¹²⁵	
							Feld-art ¹²²	Besondere Belegungsvorschriften	Feld-art ¹²²	Besondere Belegungsvorschriften
27	2	767	num	Erweiterungskennzeichen	00 = es folgt kein Meldeteil 01 – 08 = Anzahl der Meldeteile à 256 Bytes	P	N		P	
	768									

Datensatz V (Meldedatensatz für Transithandel)

Feld	Länge in Bytes	1. Stelle im Satz	Feld art ¹²⁷	Daten-format ¹²⁸	Inhalt	Erläuterungen
1	4	1	P	binär/num	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlengthen (binär bei Magnetbandkassetten, numerisch bei Disketten)
2	1	5	P	alpha	Satzart	Konstante "V"
3	27	6	P	alpha	Warenbezeichnung der eingekauften Transithandelsware	
4a	2	33	P	num	Kapitel-Nummer des Warenverzeichnisses für die eingekaufte Transithandelsware	Gemäß Warenverzeichnis für die Außenhandelsstatistik.
4b	7	35	P	num	"0000000"	Konstante "0000000"
5	7	42	P	alpha	Einkaufsland Transithandel	Kurzbezeichnung gemäß Länderverzeichnis für die Zahlungsbilanzstatistik
6	3	49	P	alpha	Ländercode für Einkaufsland Transithandel	2-stelliger ISO-alpha-Ländercode gemäß Länderverzeichnis für die Zahlungsbilanzstatistik; linksbündig zu belegen; 3. Stelle Leerzeichen
7	12	52	P	num	Einkaufspreis Transithandel (Vorkommastellen)	Angabe in Auftragswährung (siehe Feld T13); Feld T18 mit '95' belegen. ¹²⁹ Bei Euro-Gegenwertzahlungen : Angabe in Euro und Feld T19 mit '91' belegen

¹²⁷ K = Kannfeld, P = Pflichtfeld, K/P = Pflichtfeld in Abhängigkeit von bestimmten Kriterien, N = nicht belegbares Feld

¹²⁸ alpha = alphanummerische Daten (linksbündig, nicht belegte Stellen: Leerzeichen), num = numerische Daten (rechtsbündig, nicht belegte Stellen: Nullen)

¹²⁹ Die Kennzeichnung ,95' entfällt ab 1.1.2005.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Feld art 127	Daten- for- mat ¹²⁸	Inhalt	Erläuterungen
8	1	64	P	alpha	Verkauf der Transithandelsware an Gebietsfremde (durchgehandeltes Transithan- delsgeschäft)	Ja (= J) bzw. Nein (= N)
9	1	65	P	alpha	Kennzeichnung Verkauf der Transithandelsware an Gebiets- ansässige (gebrochenes Transithandels- geschäft)	Ja (= J) bzw. Nein (= N)
10	1	66	N	alpha		Reserve
11	1	67	P	alpha	Kennzeichnung Transithandels- ware unverkauft auf Lager im Ausland	Ja (= J) bzw. Nein (= N)
12	27	68	K/P	alpha	Warenbezeichnung der ver- kauften Transithandelsware	Nur belegt, wenn durchgehandelter Transithandel (J in Feld V8) und nicht identisch mit Feld V3
13a	2	95	K/P	num	Kapitel-Nummer des Warenver- zeichnisses 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 V4a
13b	7	97	P	num	"0000000"	Konstante "0000000"
14	4	104	K/P	alpha	Fälligkeit Verkaufserlös Transi- thandel	Nur belegt, wenn durchgehandelter Transithandel (J in Feld V8), Format: JJMM
15	7	108	K/P	alpha	Käuferland Transithandel	Kurzbezeichnung gemäß Länderverzeichnis für die Zahlungsbilanzstatistik; nur belegt, wenn durchgehandelter Transithandel (J in Feld V8)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Feld art 127	Daten- for- mat ¹²⁸	Inhalt	Erläuterungen
16	3	115	K/P	alpha	Ländercode für Käuferland	2-stelliger ISO-alpha-Ländercode gemäß Länderverzeichnis für die Zahlungsbilanzstatistik; linksbündig zu belegen; 3. Stelle Leerzeichen; nur belegt, wenn durchgehandelter Transithandel (J in Feld V8)
17	12	118	K/P	num	Verkaufspreis Transithandel (Vorkommastellen)	Nur belegt, wenn durchgehandelter Transithandel (J in Feld V8); Angabe in Auftragswährung (siehe Feld T13); Feld T18 mit '95' belegen. ¹³⁰ Bei Euro-Gegenwertzahlungen : Angabe in Euro und Feld T19 mit '91' belegen
18	40	130	K/P	alpha	Ergänzungsangaben Transithandel	Name und Sitz des Nachkäufers bei gebrochenem Transithandel (J in Feld V9)
19	87	170	N	alpha		Reserve
	256					

¹³⁰ Die Kennzeichnung ,95' entfällt ab 1.1.2005.

Datensatz W (Meldedatensatz für Dienstleistungen, Übertragungen und Kapitaltransaktionen)

Feld	Länge in Bytes	1. Stelle im Satz	Feldart ¹³¹	Datenformat ¹³²	Inhalt	Erläuterungen
1	4	1	P	binär/num	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlengthen (binär bei Magnetbandkassetten, numerisch bei Disketten)
2	1	5	P	alpha	Satzart	Konstante "W"
3	1	6	P	num	Belegart	Dienstleistungen, Übertragungen = '2' Kapitaltransaktionen und Kapitalerträge = '4'
4	3	7	P	num	Kennzahl	Gemäß Leistungsverzeichnis (Anlage LV zur AWV)
5	7	10	P	alpha	Land	Kurzbezeichnung gemäß Länderverzeichnis für die Zahlungsbilanzstatistik (siehe Anhang 3, Abschnitt E)
6	3	17	P	alpha	Ländercode	2-stelliger ISO-alpha-Ländercode gemäß Länderverzeichnis für die Zahlungsbilanzstatistik (siehe Anhang 3, Abschnitt E) ; linksbündig zu belegen; 3. Stelle Leerzeichen
7	7	20	K/P	alpha	Anlageland bei Kapitalverkehr	Kurzbezeichnung gemäß Länderverzeichnis für die Zahlungsbilanzstatistik ¹³³
8	3	27	K/P	alpha	Ländercode für Anlageland	2-stelliger ISO-alpha-Ländercode gemäß Länderverzeichnis für die Zahlungsbilanzstatistik ¹³³ ; linksbündig zu belegen; 3. Stelle Leerzeichen

¹³¹ K = Kannfeld, P = Pflichtfeld, K/P = Pflichtfeld in Abhängigkeit von bestimmten Kriterien, N = nicht belegbares Feld

¹³² alpha = alphanummerische Daten (linksbündig, nicht belegte Stellen: Leerzeichen), num = numerische Daten (rechtsbündig, nicht belegte Stellen: Nullen)

¹³³ Kann leer gelassen werden, wenn die Felder 5 und 6 gemäß Anhang 3, Abschnitt E, belegt sind.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld	Länge in Bytes	1. Stelle im Satz	Feldart ¹³¹	Datenformat ¹³²	Inhalt	Erläuterungen
9	12	30	P	num	Betrag für Dienstleistungen, Kapitalverkehr, Sonstiges (Vorkommastellen)	Angabe in Auftragswährung (siehe Feld T13); Feld T18 mit '95' belegen. ¹³⁴ Bei Euro-Gegenwertzahlungen : Angabe in Euro und Feld T19 mit '91' belegen
10	140	42	P	alpha	nähere Angaben zur zugrunde liegenden Leistung	Wichtige Einzelheiten des Grundgeschäfts
11	75	182	N	alpha		Reserve
	256					

¹³⁴ Die Kennzeichnung ,95' in Feld T18 entfällt ab 1.1.2005.

Datensatz Z (Datei-Nachsatz)

Der Datei-Nachsatz dient der Abstimmung. Er ist pro logischer Datei nur einmal vorhanden.

Feld	Länge in Bytes	1. Stelle im Satz	Feld- art ¹³⁵	Daten- for- mat ¹³⁶	Inhalt	Erläuterungen
1	4	1	P	binär / num	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlänge (binär bei Magnetbandkassetten, numerisch bei Disketten)
2	1	5	P	alpha	Satzart	Konstante "Z"
3	15	6	P	num	Summe aller Beträge (nur Vorkommastellen)	Summe der Betragsangabe in Feld T14a (über alle Währungen)
4	15	21	P	num	Anzahl der Datensätze T	
5	221	36	N	alpha		Reserve
	256					

¹³⁵ K = Kannfeld, P = Pflichtfeld, K/P = Pflichtfeld in Abhängigkeit von bestimmten Kriterien, N = nicht belegbares Feld

¹³⁶ alpha = alphanummerische Daten (linksbündig, nicht belegte Stellen: Leerzeichen), num = numerische Daten (rechtsbündig, nicht belegte Stellen: Nullen)

Anhang 1: Schlüssel zur Kennzeichnung der Zahlungsart

zwischenbetrieblich festgelegt	00 =	Standardübermittlung (z. B. briefliche, SWIFT-Normal)	
	10 =	Telex-Zahlung oder SWIFT-Eilig	
	11 =	Taggleiche Eilüberweisung in Euro (EUE-Überweisung) ¹³⁷	
	13 =	EU-Standardüberweisung, d.h. eine grenzüberschreitende Überweisung gemäß Artikel 2 a) i) der Verordnung Nr. 2560/2001 des Europäischen Parlaments und des Rates der Europäischen Union über grenzüberschreitende Überweisungen in Euro, die in Euro bis zu einem Betrag von 12.500 Euro lautet und bei der laut Artikel 5 (2) die IBAN des Begünstigten und der BIC des Kreditinstitutes des Begünstigten anzugeben sind.	
	15 =	Grenzüberschreitende Überweisung gemäß bilateraler Absprache mit dem Kreditinstitut	
	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	
innerbetrieblich	34	42	
	35	43	
	36	44	
	37	45	
	38	46	zunächst frei
	39	47	
	40	48	
	41	49	
innerbetrieblich	50	62	
	51	63	
	52	64	
	53	65	
	54	66	
	55	67	
	56	68	
	57	69	
	58	70	
	59	bis	
	60	99	
	61		

¹³⁷ Bitte beachten Sie die besonderen Cut-off-Zeiten für EUE-Zahlungen.

Anhang 2: Weisungsschlüssel Zahlungen**Ausprägung**

Schlüssel DTAZV	Abkürzung SWIFT - MT103	Klartext	Nicht kombinierbar mit den folgenden Weisungsschlüsseln
01	BONL	Payment is to be made to the beneficiary customer only. <i>Nur an Begünstigten zahlen.</i>	11, 12
02	CHQB	Pay beneficiary customer only by cheque. The optional account number. line in field 59 (MT103) must not be used <i>Nur mittels Scheck zahlen.</i>	04, 11, 12
04	HOLD	Beneficiary customer/claimant will call; pay upon identification. <i>Nur nach Identifikation zahlen.</i>	02, 11, 12
06	PHON	Please advise account with institution by phone. <i>Bank des Begünstigten per Telefon avisieren.</i>	07
07	TELE	Please advise account with institution by the most efficient means of telecommunication. <i>Bank des Begünstigten auf effektivste Weise per Telekommunikation avisieren.</i>	06
09	PHOB	Please advise/contact beneficiary/claimant by phone. <i>Begünstigten per Telefon avisieren.</i>	10
10	TELB	Please advise/contact beneficiary/claimant by the most efficient means of telecommunication <i>Begünstigten auf effektivste Weise per Telekommunikation avisieren.</i>	09
11	CORT	Payment is made in settlement of a trade, eg, foreign exchange deal, securities transaction. <i>Deckung z.B. für Devisen- oder Wertpapier-Geschäft.</i>	01, 02, 04
12	INTC	The payment is an intra-company payment, ie, a payment between two companies belonging to the same group. <i>Konzern-interne Zahlung.</i>	01, 02, 04
91		Euro - Gegenwertzahlung (Verwendung ist nur in Feld T 19 zugelassen, siehe Anhang 2a)	
95		Beträge in den Datensätzen V bzw. W in Auftragswährung; (Dies ist Pflicht, wenn zu einer Zahlung Meldedatensätze V bzw. W erstellt werden und die Zahlung keine Euro-Gegenwertzahlung ist. Verwendung ist nur in Feld T 18 zugelassen, siehe Anhang 3, Abschnitt D; Weisungsschlüssel entfällt ab 1.1.2005)	

Anhang 2a: Weisungsschlüssel für "Euro-Gegenwertzahlungen"

(Nicht erlaubt bei EU-Standardüberweisungen und taggleichen Eilüberweisungen in Euro (EUE-Überweisungen), d.h.: bei Zahlungsartschlüssel ,13‘ oder ,11‘ in Feld T22)

Die Weisung "Euro-Gegenwertzahlung" kann nur im Feld T19 erteilt werden.

T19 = 91 = Euro-Gegenwertzahlung

Der in den Feldern T14a und T14b angegebene Betrag ist der Euro-Betrag, der in die in Feld T13 angegebene Währung konvertiert und in dieser Währung an den Begünstigten bzw. Scheckempfänger gezahlt wird.

Eine Euro-Gegenwertzahlung kann nur zu Lasten eines Euro-Kontos erfolgen.

Anhang 3: Erläuterungen der Deutschen Bundesbank zu beleglosen Zahlungen 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, Meldefreigrenze und Aufbewahrungsfrist

1. Zu melden sind Zahlungen von Gebietsansässigen über gebietsansässige Kreditinstitute:

- an Gebietsfremde auf Auslandskonten;
- an Gebietsfremde auf Inlandskonten; (Meldung auch auf AWV-Vordruck Z4 möglich)
- für Rechnung von Gebietsfremden an Gebietsansässige; (Meldung auch auf AWV-Vordruck Z4 möglich)
- 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 **12.500 Euro** oder Gegenwert;
- Zahlungen, die **nur Wareneinfuhren** betreffen;
- Auszahlungen oder Rückzahlungen von Krediten und Einlagen mit einer vereinbarten Laufzeit bis zu 12 Monaten.
Zinsen aus diesen Geschäften sind meldepflichtig;
- Zahlungen zwischen Gebietsfremden und deren Weiterleitung durch Gebietsansässige.

3. Die Meldungen¹³⁸ sind 3 Jahre lang in einer vom Meldepflichtigen wählbaren Form aufzubewahren. Die aufbewahrten Daten müssen ggf. in eine lesbare Darstellung überführt werden können.

B. Abgabe der Meldung (Feld 9 des Datensatzes Q)

Bei meldepflichtigen Zahlungen für Dienstleistungen, Übertragungen, Kapitalverkehrstransaktionen sind grundsätzlich sowohl bei Datenträgeraustausch als auch bei Datenfernübertragung Datensätze W zu belegen und zusammen mit dem Zahlungsauftrag (Datensätze Q und T) beim beauftragten Kreditinstitut einzureichen. Zahlungen im Transithandel sollen gesammelt mit Vordruck Z4 bzw. mit entsprechenden Datensätzen gemeldet werden. Sie können

¹³⁸ Dies ist der Inhalt der Datensätze V, W und Q (ohne Feld Q4) sowie der Felder 3, 5, 8, 9a, 9b, 10a, 10b, 13, 14a, 14b, 15, 16, 17, 18, 19 und 24 - 27 des Datensatzes T

auch einzeln mit dem Datensatz V in diesem Datenträgersaustausch 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)
Zahlungen an Gebietsfremde auf Inlandskonten	Z4 (wahlweise)
Zahlungen für Rechnung von Gebietsfremden an Gebietsansässige	Z4 (wahlweise)

Das Feld 9 des Datensatzes Q muss mit 'J' belegt werden, wenn die Datei mindestens einen Meldedatensatz (V oder W) enthält.

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)

Die Beträge in den Meldedatensätzen V und W müssen ab 1.7.2003 in der in Feld T13 genannten Auftragswährung angegeben werden; zugleich muss in Feld T18 *bis zum 31.12.2004* die Kennzeichnung ,95' eingetragen werden.

Bei Euro-Gegenwertzahlungen sind die Beträge in den Meldedatensätzen prinzipiell in Euro anzugeben.

Die Möglichkeiten für die Währung in den Meldedatensätzen und deren Kennzeichnung sind in folgender Tabelle zusammengestellt:

Zahlungstyp	Meldewährung	Spezielle Belegung von T18	Spezielle Belegung von T19
Euro-Gegenwertzahlung	Euro		'91'
Sonstige Zahlung	Auftragswährung T13	'95' ¹³⁹	

¹³⁹ bis zum 31.12.2004

E. Erläuterungen zu einzelnen Positionen

Transithandel (Datensatz V) siehe B.

Mit dem Kaufpreis sollte gleichzeitig der Eingang bzw. der voraussichtliche Eingang der Zahlung angezeigt werden.

Zahlungen für Dienstleistungen, Übertragungen, Kapitaltransaktionen und den Sonstigen Warenverkehr (Datensatz W)

Die Leistungen, die der Zahlung zugrunde liegen, sind in Feld 10 des Datensatzes W ausführlich und aussagefähig zu beschreiben.

Bei Wertpapiergeschäften ist die genaue Wertpapierbezeichnung, möglichst mit der Wertpapier-Kenn-Nummer oder ISIN (laut Verlag Wertpapier-Mitteilungen), anzugeben.

Kennzahl (Feld 4 des Datensatzes W)

Für die Kennzahl gilt das Leistungsverzeichnis (Anlage LV zur AWV) sowie das Verzeichnis über die erweiterten Kennzahlen. Hinweise finden Sie in der Homepage der Deutschen Bundesbank (www.Bundesbank.DE -> Meldewesen -> Außenwirtschaft -> Schlüsselverzeichnis -> Spezielles Verzeichnis ausgewählter Kennzahlen für die Statistik des Zahlungsverkehrs mit fremden Wirtschaftsgebieten für ausgehende Zahlungen im DTAZV).

Falls Sie keine zutreffende Kennzahl (Leistungsart) finden, setzen Sie bitte die Sammelkennzahl 900 ein und beschreiben Sie die zugrunde liegende Leistung in Feld 10 des Datensatzes W detailliert.

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 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 Ausland**: Land der Baustelle
- bei **unentgeltlichen Zuwendungen** (Schenkungen): Land des Begünstigten.

Gegebenenfalls ist anstelle des Landes der Name der Internationalen Organisation in Abkürzung einzusetzen.

F. Zahlungen für Wareneinführen

Zahlungen, die nur Wareneinführen betreffen, sind **nicht** meldepflichtig.

Sofern Zahlungen außer Wareneinführen jedoch auch **meldepflichtige Sachverhalte** betreffen, gilt Abschnitt B.

Zu beachten ist, dass **Nebenleistungen im Warenverkehr**, wie z. B. Rabatte bei Exporten, Kennzahl 600, auch weiterhin **meldepflichtig** sind.

G. Telefon/Durchwahl (Feld 24 des Datensatzes T)

Mit der Angabe der Telefon-Nummer ermöglichen Sie der Bundesbank, Rückfragen schnell mit Ihnen zu klären.

H. Auskünfte, Informationsmaterial und Vordrucke

Informationsmaterial finden Sie in der Homepage der Deutschen Bundesbank (www.Bundesbank.DE -> Meldewesen -> Außenwirtschaft -> Meldungen Z1, Z4). Außerdem erhalten Sie Auskünfte und Informationsmaterial bei der Deutschen Bundesbank unter ☎ 0800-1234 111 (entgeltfrei)

Anhang 4: Zulässige Länder für EU-Standardüberweisungen

Land	ISO-Ländercode	Land	ISO-Ländercode
Österreich	AT	Griechenland	GR
Belgien	BE	Irland	IE
Dänemark	DK	Italien	IT
Spanien einschließlich Kanarische Inseln	ES	Luxemburg	LU
Finnland	FI	Martinique	MQ
Frankreich	FR	Niederlande	NL
Vereinigtes Königreich von Großbritannien und Nordirland	GB	Portugal einschließlich Azoren und Madeira	PT
Französisch Guyana	GF	Réunion	RE
Gibraltar	GI	Schweden	SE
Guadeloupe	GP		

Der BIC der Bank des Begünstigten enthält an den Stellen 5-6 einen der vorstehenden ISO-Ländercodes.

3.3 Wertpapiergeschäft

Für alle SWIFT-Formate gilt, soweit nicht anders definiert, der SWIFT-Zeichensatz:

Der SWIFT-Zeichensatz ist ein Subset von ISO 8859:

	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	ç	£	¤	¥	¦	§	¨	©	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

Die geschweiften Klammern gehören zwar zum Zeichensatz und sind als Feldbegrenzungen zulässig, dürfen aber nicht im Text einer Nachricht von Benutzer zu Benutzer verwendet werden.

3.3.1 MT 513 Ausführungsanzeige

„Client Advice of Execution“; basiert auf SWIFT „Standards Release Guide“, Stand: Oktober 1998

- **Übersicht** (ohne konstante Felder)

Folge	Sub-folge	Tag	Sta-tus ¹⁴⁰	Inhalt
A			M	Allgemeine Information
		:98C:	K	Datum/Uhrzeit zu dem die Nachricht erstellt wurde
B			K	Teilerfüllung und/oder Einzelheiten über Recap
	B1		K	Einzelheiten über Teilerfüllung
		:36B:	M	Stückzahl des Wertpapiers, bei dem ein Teilkauf oder Teilverkauf bestätigt wird
		:90a:	M	Abschlusskurs/Handelspreis des Teilgeschäfts (angegeben als Betrag oder Prozentsatz)
		:22F:	K	Art des Preises, die im Abschlusskurs bezeichnet wird

¹⁴⁰ M = Pflichtfeld, K = Kannfeld

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Sta- tus 140	Inhalt
		:98C:	K	Datum/Uhrzeit des Handels
		:94B:	K	Börsenplatz, an dem der Teilhandel ausgeführt werden soll bzw. ausgeführt wurde
		:36B:	M	Gesamte geordnete Stückzahl
		:36B:	M	Stückzahl, die bereits vorher ausgeführt wurde
		:36B:	M	Stückzahl, die als Auftrag übrig bleibt
C			M	Einzelheiten über die Order
		:98a:	M	Datum/Uhrzeit des Handels
		:90a:	M	Abschlusskurs/Handelspreis (angegeben als Betrag oder Prozentsatz)
		:99A:	K	Anzahl der aufgelaufenen Tage, die für die Berechnung des Betrages der aufgelaufenen Zinsen benutzt wird
		:94B:	K	Börsenplatz, an dem die Order gehandelt wurde
		:22H:	M	Kauf/Verkauf
		:22F:	K	Art des Preises
		:22F:	K	Bedingungen der Handelstransaktion
	C1		M	Parteien bei der Bestätigung
		:95Q:	M	Identifikation des ausführenden Instituts (Feld braucht vom Kundensystem nicht ausgewertet zu werden)
		:97A:	K	Depotkonto des Kunden
		:97A:	K	Geld-/Verrechnungskonto des Kunden
		:70E:	K	Zusätzliche Informationen über die Ausführung
		:36B:	M	Stückzahl des Wertpapiers
	:35B:	M	Referenznummer (ISIN bzw. WKN) und Gattungsbezeichnung des Wertpapiers	
	C2		K	Attribute für das Finanzinstrument
		:22F:	K	Methode der Zinsberechnung
		:22F:	K	Art der Wertpapiere
		:22F:	K	Häufigkeit der Zahlung
		:22F:	K	Vorzüge bei den Erträgen
		:22F:	K	Status der Zahlung
		:22F:	K	Beschränkungen
		:11A:	K	Währung des Nennwertes (Währung, in der die Stückzahl des Wertpapiers als Nennbetrag in C1, Feld :36B: angegeben wird)
		:98A:	K	Termine: <ul style="list-style-type: none">• Nächster Kupontermin• Verfallsdatum• Reset-Datum für eine Floating Rate Note• Fälligkeitstermin• Ausgabedatum (Emissionsdatum des Wertpapiers)• Kündigungstermin• Umtauschdatum• Put-Datum• Termin, von dem ab ein festverzinsliches Papier Zinsen trägt)
		:92A:	K	Faktoren und Zinssätze bei verzinslichen Wertpapieren
		:13B:	K	<ul style="list-style-type: none">• Kuponnummer• Pool-Nummer• Anteil-Nummer

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub-folge	Tag	Sta-tus ¹⁴⁰	Inhalt
				• Versionsnummer des Options-Kontraktes oder der Tranche
		:70E:	K	Zusätzliche Informationen zum Wertpapier (z.B. Depotart, Verwahrungsart, Depotschlüssel)
		:13B:	K	Stückenummer des Wertpapiers

• Belegungsrichtlinien

Folge	Sub-folge	Tag	Name	For-mat ¹⁴¹	Län-ge	Sta-tus ¹⁴²	An-zahl	Inhalt/Bemerkungen
A			Allgemeine Information			M	1	
A		:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R.“
			Code	c	..16	M	1	„GENL“
A		:20C:	Referenz des Senders			M	1	
			Tag			M	1	„:20C.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„SEME“
			Konstante			M	1	„/“
			Referenz	x	..16	M	1	„NONREF“
A		:23G:	Funktion der Nachricht			M	1	
			Tag			M	1	„:23G.“
			Funktion	c	4	M	1	„NEWM“
A		:98C:	Erstellungsdatum/-uhrzeit			K	1	
			Tag			M	1	„:98C.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PREP“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Uhrzeit	n	6	M	1	hhmmss
A		:22F:	Indikator: Transaktionstyp eines Handels			M	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TRTR“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„TRAD“
	A1		Verknüpfungen			K	1	
	A1	:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R.“

¹⁴¹ a = alpha (erlaubt sind „A“-„Z“), c = character (erlaubt sind „A“-„Z“ und „0“-„9“), d = dezimal (Fließkommazahl, der Vorkommaanteil muss wenigstens ein Zeichen enthalten, ein Dezimalkomma ist Pflicht und in der maximalen Länge enthalten), n = numerisch (erlaubt sind die Ziffern 0-9), x = alphanummerisch (erlaubt sind alle Zeichen aus dem SWIFT-Zeichensatz)

¹⁴² M = Pflichtfeld, K = Kannfeld

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 141	Län- ge	Sta- tus 142	An- zahl	Inhalt/Bemerkungen
	A1		Code	c	..16	M	1	„LINK“
		:20C:	Referenz des Senders			M	1	
			Tag			M	1	„:20C:“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„RELA“
			Konstante			M	1	„/“
			Referenz	x	..16	M	1	„0000000000000000“
	A1	:16S:	Blockende			M	1	
			Tag			M	1	„:16S:“
			Code	c	..16	M	1	„LINK“
		:16S:	Blockende			M	1	
			Tag			M	1	„:16S:“
			Code	c	..16	M	1	„GENL“
B			Teilerfüllung und/oder Einzelheiten über Recap			K	1	nur bei Teilausführung zu belegen Ist eine Order bereits teil- ausgeführt und kommt es zur Ausführung der restli- chen Order, so ist dieser Rest wie eine Teilausfüh- rung zu behandeln; d.h. bei der Restausführung sind im B-Teil immer alle bisherigen Teilausführun- gen und im C-Teil die Ein- zelheiten zur Gesamt- order aufzuführen.
	B	:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R:“
			Code	c	..16	M	1	„RCAP“
	B1		Einzelheiten über Teiler- füllung			K	1..n	
	B1	:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R:“
			Code	c	..16	M	1	„PAFILL“
	B1	:36B:	Stückzahl des Finanzin- struments bei Teilerfüllung			M	1	
			Tag			M	1	„:36B:“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PAFI“
			Konstante			M	1	„/“
			Typ	c	4	M	1	„FAMT“ = Die Stückzahl wird als Nennbetrag aus- gedrückt „UNIT“ = Die Stückzahl wird als Zahl (Zähler) ausgedrückt
			Konstante			M	1	„/“
			Stückzahl	d	..15	M	1	
	B1	:90a:	Abschlusskurs/Handels-			M	1	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 141	Län- ge	Sta- tus 142	An- zahl	Inhalt/Bemerkungen
			preis des Teilgeschäfts					
			Option A:					falls der Preis ein Pro- zentsatz ist
			Tag			M	1	„90A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„DEAL“
			Konstante			M	1	„/“
			Typ	c	4	M	1	„PRCT“
			Konstante			M	1	„/“
			Preis	d	..15	M	1	Die Anzahl der Nachkom- mastellen wird nicht ge- gen die Währung geprüft.
			Option B:					falls der Preis ein Betrag ist
			Tag			M	1	„90B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„DEAL“
			Konstante			M	1	„/“
			Typ	c	4	M	1	„ACTU“
			Konstante			M	1	„/“
			Währung	a	3	M	1	ISO 4217-Währungscode
			Preis	d	..15	M	1	Die Anzahl der Nachkom- mastellen wird nicht ge- gen die Währung geprüft.
	B1	:22F:	Indikator: Art des Preises			K	1	
			Tag			M	1	„22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PRIC“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„AVER“ = Preis in B1:90a: ist ein durchschnittlicher Ausführungspreis bei Teilausführung „NET1“ = Preis in B1:90a: ist ein Nettopreis, d.h. ohne Gebühren, Spesen, Steuern
	B1	:98C:	Datum/Uhrzeit des Han- dels			K	1	
			Tag			M	1	„98C.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TRAD“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Uhrzeit	n	6	M	1	hhmmss
	B1	:94B:	Ort des Handels			K	1	Börsenplatz
			Tag			M	1	„94B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TRAD“

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 141	Län- ge	Sta- tus 142	An- zahl	Inhalt/Bemerkungen
B	B1		Konstante			M	1	„/“
			Ort	c	4	M	1	„EXCH“ = Der Handelsort ist eine Börse (bei börslich gehandelten Wertpapieren) „OTCO“ = Der Handelsort ist außerbörslich (Over the Counter) (z.B. bei Investmentfonds)
			Konstante			M	1	„/“
			Freier Text	x	..30	M	1	Bei EXCH, muss der Freie Text den Kennungscode einer Börse bezeichnen (MIC). Bei OTCO Name des Systems (wenn bekannt) bzw. „AUSSERBOERS- LICH“ (wenn Name nicht bekannt oder Festpreis- geschäft) oder „SUBSC- RIPTION“ (bei Zeichnung)
		:16S:	Blockende			M	1	
			Tag			M	1	„:16S.“
			Code	c	..16	M	1	„PAFILL“
		:36B:	Stückzahl des Finanzin- strumentes			M	1	Gesamte geordnete Stückzahl
			Tag			M	1	„:36B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„ORDR“
			Konstante			M	1	„/“
			Typ	c	4	M	1	„FAMT“ = Die Stückzahl wird als Nennbetrag aus- gedrückt „UNIT“ = Die Stückzahl wird als Zahl (Zähler) ausgedrückt
			Konstante			M	1	„/“
			Stückzahl	d	..15	M	1	
		:36B:	Stückzahl des Finanzin- strumentes			M	1	Stückzahl, die bereits vorher ausgeführt wurde
			Tag			M	1	„:36B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PREX“
			Konstante			M	1	„/“
			Typ	c	4	M	1	„FAMT“ = Die Stückzahl wird als Nennbetrag aus- gedrückt „UNIT“ = Die Stückzahl wird als Zahl (Zähler) ausgedrückt
			Konstante			M	1	„/“
			Stückzahl	d	..15	M	1	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 141	Län- ge	Sta- tus 142	An- zahl	Inhalt/Bemerkungen
B		:36B:	Stückzahl des Finanzin- strumentes			M	1	Stückzahl, die als Auftrag übrig bleibt
			Tag			M	1	„:36B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„REMA“
			Konstante			M	1	„/“
			Typ	c	4	M	1	„FAMT“ = Die Stückzahl wird als Nennbetrag aus- gedrückt „UNIT“ = Die Stückzahl wird als Zahl (Zähler) ausgedrückt
			Konstante			M	1	„/“
			Stückzahl	d	..15	M	1	
B		:16S:	Blockende			M	1	
			Tag			M	1	„:16S.“
			Code	c	..16	M	1	„RCAP“
C			Einzelheiten über die Or- der			M	1	
C		:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R.“
			Code	c	..16	M	1	„ORDRDET“
C		:98a:	Datum/Uhrzeit			M	1	Datum/Uhrzeit des Han- dels
			Option A:					falls Teilausführungen innerhalb eines Tages vorliegen
			Tag			M	1	„:98A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TRAD“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Option B:					falls Teilausführungen an mehreren Tagen vorliegen
			Tag			M	1	„:98B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TRAD“
			Konstante			M	1	„/“
			Datum-Code	c	4	M	1	„VARI“
			Option C:					falls keine Teilausführung vorliegt
			Tag			M	1	„:98C.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TRAD“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Uhrzeit	n	6	M	1	hhmmss

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 141	Län- ge	Sta- tus 142	An- zahl	Inhalt/Bemerkungen
C		:90a:	Abschlusskurs/Handels- preis			M	1	falls Teilausführungen vorliegen, kann hier ent- weder ein Durchschnitts- preis oder der Wert '0,' angegeben werden.
			Option A:					falls der Preis ein Pro- zentsatz ist
			Tag			M	1	„:90A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„DEAL“
			Konstante			M	1	„/“
			Typ	c	4	M	1	„PRCT“
			Konstante			M	1	„/“
			Preis	d	..15	M	1	Die Anzahl der Nachkom- mastellen wird nicht ge- gen die Währung geprüft.
			Option B:					falls der Preis ein Betrag ist
			Tag			M	1	„:90B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„DEAL“
			Konstante			M	1	„/“
			Typ	c	4	M	1	„ACTU“
			Konstante			M	1	„/“
			Währung	a	3	M	1	ISO 4217-Währungscode
			Preis	d	..15	M	1	Die Anzahl der Nachkom- mastellen wird nicht ge- gen die Währung geprüft.
C		:99A:	Anzahl der aufgelaufenen Tage			K	1	
			Tag			M	1	„:99A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„DAAC“
			Konstante			M	1	„/“
			Vorzeichen	a	1	K	1	„N“ (nur wenn die Anzahl der Tage negativ ist)
			Nummer	n	3	M	1	ggf. mit führenden Nullen auffüllen
C		:94B:	Ort des Handels			K	1	Börsenplatz (falls Teilausführungen an verschiedenen Börsen- plätzen stattgefunden haben, wird das Feld nicht belegt)
			Tag			M	1	„:94B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TRAD“
			Konstante			M	1	„/“
			Ort	c	4	M	1	„EXCH“ = Der Handelsort ist eine Börse (bei börslich

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 141	Län- ge	Sta- tus 142	An- zahl	Inhalt/Bemerkungen
C								gehandelten Wertpapieren) "OTCO" = Der Handelsort ist außerbörslich (Over the Counter) (z.B. bei Investmentfonds)
			Konstante			M	1	„/“
			Freier Text	x	..30	M	1	Bei EXCH, muss der Freie Text den Kennungscode einer Börse bezeichnen (MIC). Bei OTCO Name des Systems (wenn bekannt) bzw. „AUSSERBOERSLICH“ (wenn Name nicht bekannt oder Festpreisgeschäft) oder „SUBSCRIPTION“ (bei Zeichnung)
	:22H:		Indikator: Kauf/Verkauf			M	1	
			Tag			M	1	„:22H.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„BUSE“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„BUY“ = Kauf „SELL“ = Verkauf
	:22F:		Indikator: Art des Preises			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PRIC“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„AVER“ = Preis in C:90a: ist ein durchschnittlicher Ausführungspreis bei Teilausführung „NET1“ = Preis in C:90a: ist ein Nettopreis, d.h. ohne Gebühren, Spesen, Steuern
	:22F:		Indikator: Bedingungen der Handelstransaktion			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TTCO“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„CBNS“ = cum Bonus „CCPN“ = cum Kupon „CDIV“ = cum Dividende „CRTS“ = cum Bezugsr. „XBNS“ = ex Bonus „XCPN“ = ex Kupon

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 141	Län- ge	Sta- tus 142	An- zahl	Inhalt/Bemerkungen
C								„XDIV“ = ex Dividende „XRTS“ = ex Bezugsrecht
		:22H:	Indikator: Zahlungsweise			M	1	
			Tag			M	1	„:22H.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PAYM“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„APMT“
	C1		Parteien bei der Bestätigung			M	1	
	C1	:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R.“
			Code	c	..16	M	1	„CONFRTY“
	C1	:95Q:	Partei			M	1	ausführendes Institut
			Tag			M	1	„:95Q.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„INVE“
			Konstante			M	1	„/“
			Name und Anschrift	x	..35	M	1	BLZ oder BIC-Code des ausführenden Instituts
	C1	:97A:	Konto			K	1	Depotkonto
			Tag			M	1	„:97A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„SAFE“
			Konstante			M	1	„/“
			Konto	x	..35	M	1	BLZ gefolgt von „/“ und der Kontonummer
	C1	:97A:	Konto			K	1	Geld-/Verrechnungskonto
			Tag			M	1	„:97A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„CASH“
			Konstante			M	1	„/“
			Konto	x	..35	M	1	BLZ gefolgt von „/“ und der Kontonummer
	C1	:70E:	Freier Text für Einzelerklärungen			K	1	Zusätzliche Informationen über die Ausführung
			Tag			M	1	„:70E.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„DECL“
			Konstante			M	1	„/“
			Freier Text	x	..35	M	1..10	Die Zeilen werden mit <CR><LF> getrennt.
	C1	:16S:	Blockende			M	1	
			Tag			M	1	„:16S.“
			Code	c	..16	M	1	„CONFRTY“
	C	:36B:	Stückzahl des angezeigten Finanzinstruments			M	1	Wenn Teilausführungen vorliegen, ist die Summe der Teilausführungen in

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 141	Län- ge	Sta- tus 142	An- zahl	Inhalt/Bemerkungen	
C								Folge B anzugeben	
			Tag			M	1	„:36B:“	
			Konstante			M	1	„:“	
			Qualifier	c	4	M	1	„ADVI“	
			Konstante			M	1	„/“	
			Typ	c	4	M	1	„FAMT“ = Die Stückzahl wird als Nennbetrag ausgedrückt „UNIT“ = Die Stückzahl wird als Zahl (Zähler) ausgedrückt	
			Konstante			M	1	„/“	
			Stückzahl	d	..15	M	1		
			:35B:	Kennung des Finanzinstruments			M	1	Es muss entweder die ISIN oder die WKN oder beide angegeben werden.
		Tag			M	1	„:35B:“		
		Konstante			K	1	„ISIN“ (nur wenn ISIN angegeben wird)		
		Konstante			K	1	„ „ (Leerzeichen, nur wenn ISIN angegeben wird)		
		ISIN-Kennung	x	..12	M	1	Wird keine ISIN verwendet, so ist „/DE/“ gefolgt von der deutschen Wertpapierkennnummer (WKN) anzugeben.		
		Konstante			M	1	<CR><LF>		
		Freier Text	x	..35	M	1..4	Wertpapierbezeichnung Falls ISIN und WKN gemeinsam angegeben werden, ist die WKN in die erste Zeile und die Bezeichnung in die Zeilen 2-4 einzustellen. Die Zeilen werden mit <CR><LF> getrennt.		
		C2		Attribute für das Finanzinstrument			K	1	
		C2	:16R:	Blockanfang			M	1	
				Tag			M	1	„:16R:“
	Code			c	..16	M	1	„FIA“	
	C2	:22F:	Indikator: Methode der Zinsberechnung			K	1		
			Tag			M	1	„:22F:“	
			Konstante			M	1	„:“	
			Qualifier	c	4	M	1	„MICO“	
			Konstante			M	1	„/“	
			Indikator	c	4	M	1	„A001“ = 30/360 „A002“ = 30/365 „A003“ = 30/Aktuell „A004“ = Aktuell/360	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 141	Län- ge	Sta- tus 142	An- zahl	Inhalt/Bemerkungen
								„A005“ = Aktuell/365 „A006“ = Aktuell/Aktuell oder 1/1 „A007“ = 30E/360 oder Eurobond Basis
	C2	:22F:	Indikator: Art der Wertpa- piere			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„FORM“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„BEAR“ = Inhaberpapier „REGD“ = Namenspapier
	C2	:22F:	Indikator: Häufigkeit der Zahlung			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PFRE“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„ANNU“ = jährlich „MNTH“ = monatlich „QUTR“ = vierteljährlich „SEMI“ = halbjährlich „WEEK“ = wöchentlich
	C2	:22F:	Indikator: Vorzüge bei den Erträgen			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PREF“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„ORDN“ = Stammaktien „PRFD“ = Das Wertpapier hat einen bevorzugten Anspruch auf Erträge und Anlagen
	C2	:22F:	Indikator: Status der Zah- lung			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PAYS“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„FULL“ = vollständig be- zahlt „NILL“ = nichts bezahlt „PART“ = teilweise be- zahlt
	C2	:22F:	Indikator: Beschränkun- gen			K	1	
			Tag			M	1	„:22F.“

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 141	Län- ge	Sta- tus 142	An- zahl	Inhalt/Bemerkungen
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„REST“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„144A“ = Nicht registrier- tes Papier nach den ge- setzlichen Beschränkun- gen 144A in den USA „NRST“ = Eigentum oder Übertragung unterliegt keinen Beschränkungen „RSTR“ = Eigentum oder Übertragung unterliegt Beschränkungen (nicht nach 144A)
		C2	:11A: Währung			K	1	Währung des Nennwerts
			Tag			M	1	„.11A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„DENO“
			Konstante			M	1	„/“
			Währung	a	3	M	1	ISO 4217-Code
		C2	:98A: Datum			K	n	Termine
			Tag			M	1	„.98A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„COUP“ = Nächster Ku- pon-Termin „EXPI“ = Verfallsdatum „FRNR“ = Reset-Datum für eine Floating Rate Note „MATU“ = Fälligkeitster- min „ISSU“ = Ausgabedatum (Emissionsdatum des Wertpapiers) „CALD“ = Kündigungster- min „CONV“ = Umtauschda- tum „PUTT“ = Put-Datum „DDTE“ = Stichtag (Ter- min, von dem ab ein fest- verzinsliches Papier Zin- sen trägt)
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
		C2	:92A: Kurs/Satz			K	n	Faktoren und Zinssätze bei verzinslichen Wertpa- piern
			Tag			M	1	„.92A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PRFC“ = Voriger Faktor

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 141	Län- ge	Sta- tus 142	An- zahl	Inhalt/Bemerkungen
								als Dezimalbruch zwischen 0 und 1, mit dem der ausstehende Hauptbetrag des Rentenpapiers definiert wird „CUFC“ = Laufender Faktor als Dezimalbruch zwischen 0 und 1, mit dem der ausstehende Hauptbetrag des Rentenpapiers definiert wird „NWFC“ = Nächster Faktor als Dezimalbruch zwischen 0 und 1, mit dem der ausstehende Hauptbetrag des Rentenpapiers definiert wird „INTR“ = Zinssatz (1. Verhältnis des während einer bestimmten Zeitperiode gezahlten Zinsbetrages zum Hauptbetrag des festverzinslichen Wertpapiers; 2. Gegenwärtiger Zinssatz eines Schuldscheins mit variabler Verzinsung) „NXRT“ = Nächster Zinssatz (bei einem Schuldschein mit variabler Verzinsung der Zinssatz, der für die nächste Zahlungsperiode gilt)
			Konstante			M	1	„/“
			Vorzeichen	a	1	K	1	„N“ (nur wenn der Betrag negativ ist)
			Kurs/Satz	d	..15	M	1	
	C2	:13B:	Numerische Kennung			K	n	
			Tag			M	1	„.13B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„COUP“ = Kupon-Nummer (Nummer des nächsten Kupons auf dem Bogen) „POOL“ = Pool-Nummer (Nummer, die vom Emittenten eines Asset-backed security (USA) vergeben wird, um die Gruppe von Grundpfandrechten zu bezeichnen) „LOTS“ = Anteil-Nummer (Numerische Kennung des Anteils einer Wertpapieremission) „VERN“ = Versions-Num-

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 141	Län- ge	Sta- tus 142	An- zahl	Inhalt/Bemerkungen
C	C2							mer des Options-Kontrak- tes oder der Tranche
			Konstante			M	1	„/“
			Nummer	x	..30	M	1	
		:70E:	Freier Text zu Eigenschaf- ten des Finanzinstruments			K	1	
			Tag			M	1	„:70E:“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„FIAN“
			Konstante			M	1	„/“
			Freier Text	x	..35	M	1.. 10	Die Zeilen werden mit <CR><LF> getrennt.
		:16S:	Blockende			M	1	
			Tag			M	1	„:16S:“
			Code	c	..16	M	1	„FIA“
	C	:13B:	Nummer des Zertifikates			K	n	
			Tag			M	1	„:13B:“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„CERT“
			Konstante			M	1	„/“
			Nummer	x	..30	M	1	Stückenummer des Wert- papiers
		:16S:	Blockende			M	1	
			Tag			M	1	„:16S:“
			Code	c	..16	M	1	„ORDRDET“

• Beispiel

Beispiel: Kauf ohne Teilausführung:

Folge	Sub-folge	Beispiel
A		:16R:GENL :20C::SEME//NONREF :23G:NEWM :98C::PREP//19990305122030 :22F::TRTR//TRAD
	A1	:16R:LINK :20C::RELA//0000000000000000 :16S:LINK
		:16S:GENL
C		:16R:ORDRDET :98C::TRAD//19990302112030 :90B::DEAL//ACTU/EUR52,7 :94B::TRAD//EXCH/XFRA :22H::BUSE//BUYI :22F::PRIC//NET1 :22F::TTCO//CBNS :22H::PAYM//APMT
	C1	:16R:CONFPRTY :95Q::INVE//10020030 :97A::SAFE//10020030/1234567 :97A::CASH//10020030/987654321 :16S:CONFPRTY
		:36B::ADVI//UNIT/50, :35B:/DE/123456 Mustermann AG, Stammaktien
	C2	:16R:FIA :22F::FORM//BEAR

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub-folge	Beispiel
		:16S:FIA
		:16S:ORDRDET
		-

Beispiel: Verkauf mit zwei Teilausführungen zum Kurs von 52 Euro bei 50 Stück und 54 Euro bei 30 Stück:

Folge	Sub-folge	Beispiel
A		:16R:GENL :20C::SEME//NONREF :23G:NEWM :98C::PREP//19990305122030 :22F::TRTR//TRAD
	A1	:16R:LINK :20C::RELA//000000000000000000 :16S:LINK
		:16S:GENL
B		:16R:RCAP
	B1	:16R:PAFILL :36B::PAFI//UNIT/50, :90B::DEAL//ACTU/EUR52, :22F::PRIC//NET1 :98C::TRAD//19990302112030 :94B::TRAD//EXCH/XFRA :16S:PAFILL
	B1	:16R:PAFILL :36B::PAFI//UNIT/30, :90B::DEAL//ACTU/EUR54, :22F::PRIC//NET1 :98C::TRAD//19990302112101 :94B::TRAD//EXCH/XFRA

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub-folge	Beispiel
		:16S:PAFILL
		:36B::ORDR//UNIT/300, :36B::PREX//UNIT/120, :36B::REMA//UNIT/100, :16S:RCAP
C		:16R:ORDRDET :98A::TRAD//19990302 :90B::DEAL//ACTU/EUR52,75 :94B::TRAD//EXCH/XFRA :22H::BUSE//SELL :22F::PRIC//AVER :22F::TTCO//CCPN :22H::PAYM//APMT
	C1	:16R:CONFPRTY :95Q::INVE//10020030 :97A::SAFE//10020030/1234567 :97A::CASH//10020030/987654321 :16S:CONFPRTY
		:36B::ADVI//UNIT/80, :35B:ISIN DE0123456789 /DE/123456 Mustermann AG, Stammaktien
	C2	:16R:FIA :22F::FORM//BEAR :13B::COUP//1234567 :16S:FIA
		:13B::CERT//1234567890 :16S:ORDRDET -

3.3.2 MT 515 Wertpapierabrechnung

„Client Confirmation of Purchase or Sale“; basiert auf SWIFT „Standards Release Guide“, Stand: Oktober 1998

- **Übersicht** (ohne konstante Felder)

Folge	Sub-folge	Tag	Sta-tus ¹⁴³	Inhalt
A			M	Allgemeine Information
		:98C:	K	Datum/Uhrzeit zu dem die Nachricht erstellt wurde
B			K	Einzelheiten über Teilerfüllung
		:36B:	M	Stückzahl des Wertpapiers, bei dem ein Teilkauf oder Teilverkauf bestätigt wird
		:90a:	M	Abschlusskurs/Handelspreis des Teilgeschäfts (angegeben als Betrag oder Prozentsatz)
		:22F:	K	Art des Preises, die im Abschlusskurs bezeichnet wird
		:98C:	K	Datum/Uhrzeit des Handels
		:94B:	K	Börsenplatz, an dem der Teilhandel ausgeführt werden soll bzw. ausgeführt wurde
C			M	Einzelheiten zur Bestätigung
		:98a:	M	Datum/Uhrzeit des Handels
		:98C:	M	Datum/Uhrzeit der Abrechnung
		:90a:	M	Abschlusskurs/Handelspreis (angegeben als Betrag bzw. Prozentsatz)
		:99A:	K	Anzahl der aufgelaufenen Tage, die für die Berechnung des Betrages der aufgelaufenen Zinsen benutzt wird
		:94B:	K	Börsenplatz, an dem die Order gehandelt wurde
		:19A:	M	Abrechnungsbetrag (inkl. Gebühren, Spesen etc.)
		:22H:	M	Kauf/Verkauf
		:22F:	K	Art des Preises
		:22F:	K	Bedingungen der Handelstransaktion
	C1		M	Parteien bei der Bestätigung
		:95Q:	M	Identifikation des ausführenden Instituts (Feld braucht vom Kundensystem nicht ausgewertet zu werden)
		:97A:	K	Depotkonto des Kunden
		:97A:	K	Geld-/Verrechnungskonto des Kunden
		:70E:	K	Zusätzliche Informationen über die Ausführung
		:36B:	M	Stückzahl des Wertpapiers
		:35B:	M	Referenznummer (ISIN bzw. WKN) und Gattungsbezeichnung des Wertpapiers
	C2		K	Attribute für das Finanzinstrument
		:22F:	K	Methode der Zinsberechnung
		:22F:	K	Art der Wertpapiere
		:22F:	K	Häufigkeit der Zahlung
		:22F:	K	Vorzüge bei den Erträgen
		:22F:	K	Status der Zahlung
		:22F:	K	Beschränkungen

¹⁴³ M = Pflichtfeld, K = Kannfeld

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub-folge	Tag	Sta-tus ¹⁴³	Inhalt
		:11A:	K	Währung des Nennwertes (Währung, in der die Stückzahl des Wertpapiers als Nennbetrag in C1, Feld :36B: angegeben wird)
		:98A:	K	Termine: <ul style="list-style-type: none"> Nächster Kupon-Termin Verfallsdatum Reset-Datum für eine Floating Rate Note Fälligkeitstermin Ausgabedatum (Emissionsdatum des Wertpapiers) Kündigungstermin Umtauschdatum Put-Datum Termin (von dem ab ein festverzinsliches Papier Zinsen trägt)
		:92A:	K	Faktoren und Zinssätze bei verzinslichen Wertpapieren
		:13B:	K	<ul style="list-style-type: none"> Kupon-Nummer Pool-Nummer Anteil-Nummer Versions-Nummer des Options-Kontraktes oder der Tranche
		:70E:	K	Zusätzliche Informationen zum Wertpapier (z.B. Depotart, Verwahrungsart, Depotschlüssel)
		:13B:	K	Stückenummer des Wertpapiers
D			K	Einzelheiten zur Abrechnung
	D3		K	Beträge
		:19A:	M	Barbeträge (Steuern, Gebühren, Spesen, Maklerprovisionen etc.)
		:98A:	K	Wertstellungsdatum (Datum, zu dem der Geldübertrag stattfinden muss)
		:92B:	K	Wechselkurs (dient zur Umrechnung von Barbeträgen aus Feld :19A: in den Sequenzen C und D3)

• Belegungsrichtlinien

Folge	Sub-folge	Tag	Name	For-mat ¹⁴⁴	Län-ge	Sta-tus ¹⁴⁵	An-zahl	Inhalt/Bemerkungen
A			Allgemeine Information			M	1	
A		:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R.“
			Code	c	..16	M	1	„GENL“
A		:20C:	Referenz des Senders			M	1	

¹⁴⁴ a = alpha (erlaubt sind „A“-„Z“), c = character (erlaubt sind „A“-„Z“ und „0“-„9“), d = dezimal (Fließkommazahl, der Vorkommaanteil muss wenigstens ein Zeichen enthalten, ein Dezimalkomma ist Pflicht und in der maximalen Länge enthalten), n = numerisch (erlaubt sind die Ziffern 0-9), x = alphanummerisch (erlaubt sind alle Zeichen aus dem SWIFT-Zeichensatz)

¹⁴⁵ M = Pflichtfeld, K = Kannfeld

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen	
A			Tag			M	1	„:20C.“	
			Konstante			M	1	„.“	
			Qualifier	c	4	M	1	„SEME“	
			Konstante			M	1	„/“	
			Referenz	x	..16	M	1	„NONREF“	
	:23G:		Funktion der Nachricht			M	1		
			Tag			M	1	„:23G.“	
			Funktion	c	4	M	1	„NEWM“	
	:98C:		Erstellungsdatum/-uhrzeit			K	1		
			Tag			M	1	„:98C.“	
			Konstante			M	1	„.“	
			Qualifier	c	4	M	1	„PREP“	
			Konstante			M	1	„/“	
			Datum	n	8	M	1	JJJJMMTT	
			Uhrzeit	n	6	M	1	hhmmss	
			:22F:		Indikator: Transaktionstyp eines Handels			M	1
Tag							M	1	„:22F.“
Konstante					M	1	„.“		
Qualifier	c	4			M	1	„TRTR“		
Konstante					M	1	„/“		
Indikator	c	4			M	1	„TRAD“		
A	A1		Verknüpfungen			M	1		
			:16R:	Blockanfang			M	1	
				Tag			M	1	„:16R.“
	Code	c		..16	M	1	„LINK“		
	:20C:		Referenz des Senders			M	1		
			Tag			M	1	„:20C.“	
			Konstante			M	1	„.“	
			Qualifier	c	4	M	1	„RELA“	
			Konstante			M	1	„/“	
			Referenz	x	..16	M	1	„0000000000000000“	
	:16S:		Blockende			M	1		
			Tag			M	1	„:16S.“	
			Code	c	..16	M	1	„LINK“	
	:16S:		Blockende			M	1		
			Tag			M	1	„:16S.“	
Code			c	..16	M	1	„GENL“		
B			Einzelheiten über Teilerfüllung			K	1..n	nur bei Teilausführung zu belegen	
B	:16R:		Blockanfang			M	1		
			Tag			M	1	„:16R.“	
			Code	c	..16	M	1	„PAFILL“	
B	:36B:		Stückzahl des Finanzinstruments bei Teilerfüllung			M	1		
			Tag			M	1	„:36B.“	
			Konstante			M	1	„.“	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen
B		:90a:	Qualifier	c	4	M	1	„PAFI“
			Konstante			M	1	„/“
			Typ	c	4	M	1	„FAMT“ = Die Stückzahl wird als Nennbetrag ausgedrückt „UNIT“ = Die Stückzahl wird als Zahl (Zähler) ausgedrückt
			Konstante			M	1	„/“
			Stückzahl	d	..15	M	1	
			Abschlusskurs/Handelspreis des Teilgeschäfts			M	1	
			Option A: falls der Preis ein Prozentsatz ist					
			Tag			M	1	„:90A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„DEAL“
			Konstante			M	1	„/“
			Typ	c	4	M	1	„PRCT“
			Konstante			M	1	„/“
			Preis	d	..15	M	1	Die Anzahl der Nachkommastellen wird nicht gegen die Währung geprüft.
			Option B: falls der Preis ein Betrag ist					
			Tag			M	1	„:90B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„DEAL“
			Konstante			M	1	„/“
			Typ	c	4	M	1	„ACTU“
			Konstante			M	1	„/“
			Währung	a	3	M	1	ISO 4217-Währungscode
			Preis	d	..15	M	1	Die Anzahl der Nachkommastellen wird nicht gegen die Währung geprüft.
B	:22F:		Indikator: Art des Preises			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PRIC“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„AVER“ = Preis in B:90a: ist ein durchschnittlicher Ausführungspreis bei Teilausführung „NET1“ = Preis in B:90a: ist ein Nettopreis, d.h. ohne Gebühren, Spesen, Steuern
B	:98C:		Datum/Uhrzeit des Handels			K	1	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen
B			Tag			M	1	„98C.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TRAD“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Uhrzeit	n	6	M	1	hhmmss
	:94B:		Ort des Handels			K	1	
			Tag			M	1	„94B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TRAD“
			Konstante			M	1	„/“
			Ort	c	4	M	1	„EXCH“ = Der Handelsort ist eine Börse (bei börslich gehandelten Wertpapie- ren) „OTCO“ = Der Handelsort ist außerbörslich (Over the Counter) (z.B. bei Investmentfonds)
			Konstante			M	1	„/“
			Freier Text	x	..30	M	1	Bei EXCH, muss der Freie Text den Kennungscode einer Börse bezeichnen (MIC). Bei OTCO Name des Systems (wenn bekannt) bzw. „AUSSERBOERS- LICH“ (wenn Name nicht bekannt oder Festpreisge- schäft) oder „SUBSCRIP- TION“ (bei Zeichnung)
B	:16S:		Blockende			M	1	
			Tag			M	1	„16S.“
			Code	c	..16	M	1	„PAFILL“
C			Einzelheiten zur Bestäti- gung			M	1	
C	:16R:		Blockanfang			M	1	
			Tag			M	1	„16R.“
			Code	c	..16	M	1	„CONFDET“
C	:98a:		Datum/Uhrzeit			M	1	Datum/Uhrzeit des Han- dels
			Option A:					falls Teilausführungen innerhalb eines Tages vorliegen
			Tag			M	1	„98A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TRAD“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Option B:					falls Teilausführungen an mehreren Tagen vorliegen

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen		
C			Tag			M	1	„98B.“		
			Konstante			M	1	„.“		
			Qualifier	c	4	M	1	„TRAD“		
			Konstante			M	1	„/“		
			Datum-Code	c	4	M	1	„VARI“		
			Option C:						falls keine Teilausführung vorliegt	
			Tag			M	1	„98C.“		
			Konstante			M	1	„.“		
			Qualifier	c	4	M	1	„TRAD“		
			Konstante			M	1	„/“		
			Datum	n	8	M	1	JJJJMMTT		
			Uhrzeit	n	6	M	1	hhmmss		
	C	:98C:	Datum/Uhrzeit			M	1	Datum/Uhrzeit der Abrechnung		
			Tag			M	1	„98C.“		
			Konstante			M	1	„.“		
			Qualifier	c	4	M	1	„SETT“		
			Konstante			M	1	„/“		
			Datum	n	8	M	1	JJJJMMTT		
			Uhrzeit	n	6	M	1	hhmmss		
:90a:		Abschlusskurs/Handelspreis			M	1	falls Teilausführungen vorliegen, kann hier entweder ein Durchschnittspreis oder der Wert '0,' angegeben werden.			
		Option A:						falls der Preis ein Prozentsatz ist		
		Tag			M	1	„90A.“			
		Konstante			M	1	„.“			
		Qualifier	c	4	M	1	„DEAL“			
		Konstante			M	1	„/“			
		Typ	c	4	M	1	„PRCT“			
		Konstante			M	1	„/“			
		Preis	d	..15	M	1	Die Anzahl der Nachkommastellen wird nicht gegen die Währung geprüft.			
		Option B:						falls der Preis ein Betrag ist		
Tag			M	1	„90B.“					
Konstante			M	1	„.“					
Qualifier	c	4	M	1	„DEAL“					
Konstante			M	1	„/“					
Typ	c	4	M	1	„ACTU“					
Konstante			M	1	„/“					
Währung	a	3	M	1	ISO 4217-Währungscode					
Preis	d	..15	M	1	Die Anzahl der Nachkommastellen wird nicht gegen die Währung geprüft.					

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen
C		:99A:	Anzahl der aufgelaufenen Tage			K	1	
			Tag			M	1	„99A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„DAAC“
			Konstante			M	1	„/“
			Vorzeichen	a	1	K	1	„N“ (nur wenn die Anzahl der Tage negativ ist)
			Nummer	n	3	M	1	ggf. mit führenden Nullen auffüllen
C		:94B:	Ort des Handels			K	1	Börsenplatz (falls Teilausführungen an verschiedenen Börsenplätzen stattgefunden haben, wird das Feld nicht belegt)
			Tag			M	1	„94B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TRAD“
			Konstante			M	1	„/“
			Ort	c	4	M	1	„EXCH“ = Der Handelsort ist eine Börse (bei börslich gehandelten Wertpapieren) „OTCO“ = Der Handelsort ist außerbörslich (Over the Counter) (z.B. bei Investmentfonds)
			Konstante			M	1	„“
C		:19A:	Betrag der Abrechnung			M	1	inkl. Gebühren, Spesen etc.
			Tag			M	1	„19A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„SETT“
			Konstante			M	1	„/“
			Vorzeichen	a	1	K	1	„N“ (nur wenn der Betrag negativ ist)
			Währungscode	a	3	M	1	ISO 4217-Code
C		:22H:	Betrag	d	15	M	1	
			Indikator: Kauf/Verkauf			M	1	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen
C			Tag			M	1	„:22H.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„BUSE“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„BUYI“ = Kauf „SELL“ = Verkauf
		:22F:	Indikator: Art des Preises			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PRIC“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„AVER“ = Preis in C:90a: ist ein durchschnittlicher Ausführungspreis bei Teilausführung „NET1“ = Preis in C:90a: ist ein Nettopreis, d.h. ohne Gebühren, Spesen, Steuern
		:22F:	Indikator: Bedingungen der Handelstransaktion			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TTCO“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„CBNS“ = cum Bonus „CCPN“ = cum Kupon „CDIV“ = cum Dividende „CRTS“ = cum Bezugsr. „XBNS“ = ex Bonus „XCPN“ = ex Kupon „XDIV“ = ex Dividende „XRTS“ = ex Bezugsrecht
		:22H:	Indikator: Zahlungsweise			M	1	
			Tag			M	1	„:22H.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PAYM“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„APMT“
	C1		Parteien bei der Bestäti- gung			M	1	
	C1	:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R.“
			Code	c	..16	M	1	„CONFPTY“
	C1	:95Q:	Partei			M	1	ausführendes Institut
			Tag			M	1	„:95Q.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„INVE“
			Konstante			M	1	„/“

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen
C	C1		Name und Anschrift	x	..35	M	1	BLZ oder BIC-Code des ausführenden Instituts
		:97A:	Konto			K	1	Depotkonto
			Tag			M	1	„:97A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„SAFE“
			Konstante			M	1	„/“
			Konto	x	..35	M	1	BLZ gefolgt von „/“ und der Kontonummer
	C1	:97A:	Konto			K	1	Geld-/Verrechnungskonto
			Tag			M	1	„:97A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„CASH“
			Konstante			M	1	„/“
			Konto	x	..35	M	1	BLZ gefolgt von „/“ und der Kontonummer
	C1	:70E:	Freier Text für Einzelerklärungen			K	1	
			Tag			M	1	„:70E.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„DECL“
			Konstante			M	1	„/“
			Freier Text	x	..35	M	1..10	Die Zeilen werden mit <CR><LF> getrennt.
	C1	:16S:	Blockende			M	1	
			Tag			M	1	„:16S.“
			Code	c	..16	M	1	„CONFRTY“
	C	:36B:	Stückzahl des bestätigten Finanzinstruments			M	1	Wenn Teilausführungen vorliegen, ist die Summe der Teilausführungen in Folge B anzugeben
			Tag			M	1	„:36B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„CONF“
			Konstante			M	1	„/“
			Typ	c	4	M	1	„FAMT“ = Die Stückzahl wird als Nennbetrag ausgedrückt „UNIT“ = Die Stückzahl wird als Zahl (Zähler) ausgedrückt
			Konstante			M	1	„/“
			Stückzahl	d	..15	M	1	
	C	:35B:	Kennung des Finanzinstruments			M	1	Es muss entweder die ISIN oder die WKN oder beide angegeben werden.
			Tag			M	1	„:35B.“
			Konstante			K	1	„ISIN“ (nur wenn ISIN angegeben wird)
			Konstante			K	1	„ „ (Leerzeichen, nur wenn

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen
								ISIN angegeben wird)
			ISIN-Kennung	x	..12	M	1	Wird keine ISIN verwen- det, so ist im Feld „Freier Text“ in der ersten Zeile „/DE/“ gefolgt von der deutschen Wertpapie- rennummer (WKN) an- zugeben.
			Konstante			M	1	<CR><LF>
			Freier Text	x	..35	M	1..4	Wertpapierbezeichnung Falls ISIN und WKN ge- meinsam angegeben wer- den, ist die WKN in die erste Zeile und die Be- zeichnung in die Zeilen 2- 4 einzustellen. Die Zeilen werden mit <CR><LF> getrennt.
	C2		Attribute für das Finanzin- strument			K	1	
	C2	:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R.“
			Code	c	..16	M	1	„FIA“
	C2	:22F:	Indikator: Methode der Zinsberechnung			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„MICO“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„A001“ = 30/360 „A002“ = 30/365 „A003“ = 30/Aktuell „A004“ = Aktuell/360 „A005“ = Aktuell/365 „A006“ = Aktuell/Aktuell oder 1/1 „A007“ = 30E/360 oder Eurobond Basis
	C2	:22F:	Indikator: Art der Wertpa- piere			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„FORM“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„BEAR“ = Inhaberpapier „REGD“ = Namenspapier
	C2	:22F:	Indikator: Häufigkeit der Zahlung			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PFRE“

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen
	C2		Konstante			M	1	„/“
			Indikator	c	4	M	1	„ANNU“ = jährlich „MNTH“ = monatlich „QUTR“ = vierteljährlich „SEMI“ = halbjährlich „WEEK“ = wöchentlich
		:22F:	Indikator: Vorzüge bei den Erträgen			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PREF“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„ORDN“ = Stammaktien „PRFD“ = Das Wertpapier hat einen bevorzugten Anspruch auf Erträge und Anlagen
		:22F:	Indikator: Status der Zahlung			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PAYS“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„FULL“ = vollständig bezahlt „NILL“ = nichts bezahlt „PART“ = teilweise bezahlt
	C2	:22F:	Indikator: Beschränkungen			K	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„REST“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„144A“ = Nicht registriertes Papier nach den gesetzlichen Beschränkungen 144A in den USA „NRST“ = Eigentum oder Übertragung unterliegt keinen Beschränkungen „RSTR“ = Eigentum oder Übertragung unterliegt Beschränkungen (nicht nach 144A)
		:11A:	Währung			K	1	Währung des Nennwerts
			Tag			M	1	„:11A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„DENO“
			Konstante			M	1	„/“

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen
			Währung	a	3	M	1	ISO 4217-Code
	C2	.98A:	Datum			K	n	Termine
			Tag			M	1	„.98A.“
			Konstante			M	1	„.“
			Qualifizier	c	4	M	1	„COUP“ = Nächster Ku- pon-Termin „EXPI“ = Verfallsdatum „FRNR“ = Reset-Datum für eine Floating Rate Note „MATU“ = Fälligkeitster- min „ISSU“ = Ausgabedatum (Emissionsdatum des Wertpapiers) „CALD“ = Kündigungster- min „CONV“ = Umtauschda- tum „PUTT“ = Put-Datum „DDTE“ = Stichtag (Ter- min, von dem ab ein fest- verzinsliches Papier Zin- sen trägt)
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
	C2	.92A:	Kurs/Satz			K	n	Faktoren und Zinssätze bei verzinslichen Wertpa- piern
			Tag			M	1	„.92A.“
			Konstante			M	1	„.“
			Qualifizier	c	4	M	1	„PRFC“ = Voriger Faktor als Dezimalbruch zwi- schen 0 und 1, mit dem der ausstehende Haupt- betrag des Rentenpapiers definiert wird „CUFC“ = Laufender Fak- tor als Dezimalbruch zwi- schen 0 und 1, mit dem der ausstehende Haupt- betrag des Rentenpapiers definiert wird „NWFC“ = Nächster Fak- tor als Dezimalbruch zwi- schen 0 und 1, mit dem der ausstehende Haupt- betrag des Rentenpapiers definiert wird „INTR“ = Zinssatz (1. Ver- hältnis des während einer bestimmten Zeitperiode gezählten Zinsbetrages

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen
C	C2	:13B:						zum Hauptbetrag des festverzinslichen Wertpapiers; 2. Gegenwärtiger Zinssatz eines Schuldscheins mit variabler Verzinsung) „NXRT“ = Nächster Zinssatz (bei einem Schuldschein mit variabler Verzinsung der Zinssatz, der für die nächste Zahlungsperiode gilt)
			Konstante			M	1	„/“
			Vorzeichen	a	1	K	1	„N“ (nur wenn der Betrag negativ ist)
			Kurs/Satz	d	..15	M	1	
			Numerische Kennung			K	n	
			Tag			M	1	„:13B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„COUP“ = Kupon-Nummer (Nummer des nächsten Kupons auf dem Bogen) „POOL“ = Pool-Nummer (Nummer, die vom Emittenten eines Asset-backed security (USA) vergeben wird, um die Gruppe von Grundpfandrechten zu bezeichnen) „LOTS“ = Anteil-Nummer (Numerische Kennung des Anteils einer Wertpapieremission) „VERN“ = Versions-Nummer des Options-Kontraktes oder der Tranche
			Konstante			M	1	„/“
			Nummer	x	..30	M	1	
		:70E:	Freier Text zu Eigenschaften des Finanzinstruments			K	1	
			Tag			M	1	„:70E.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„FIAN“
			Konstante			M	1	„/“
			Freier Text	x	..35	M	1..10	Die Zeilen werden mit <CR><LF> getrennt.
		:16S:	Blockende			M	1	
			Tag			M	1	„:16S.“
			Code	c	..16	M	1	„FIA“
	:13B:		Nummer des Zertifikates			K	n	
			Tag			M	1	„:13B.“

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen		
C			Konstante			M	1	„.“		
			Qualifier	c	4	M	1	„CERT“		
			Konstante			M	1	„/“		
			Nummer	x	..30	M	1	Stückenummer des Wert- papiers		
	:16S:		Blockende			M	1			
			Tag			M	1	„:16S.“		
			Code	c	..16	M	1	„CONFDET“		
D			Einzelheiten zur Abrech- nung			K	1			
D	:16R:		Blockanfang			M	1			
			Tag			M	1	„:16R.“		
			Code	c	..16	M	1	„SETDET“		
D	:22F:		Indikator: Art der Abrech- nungstransaktion			M	1			
			Tag			M	1	„:22F.“		
			Konstante			M	1	„.“		
			Qualifier	c	4	M	1	„SETR“		
			Konstante			M	1	„/“		
			Indikator	c	4	M	1	„TRAD“		
			:17B:		Merkmal für Ersatz von Dauer-Anweisungen			M	1	
					Tag			M	1	„:17B.“
Konstante					M	1	„.“			
Qualifier	c	4			M	1	„STAN“			
Konstante					M	1	„/“			
Merkmal	a	1			M	1	„N“			
D3			Beträge			K	n			
	D3	:16R:	Blockanfang			M	1			
			Tag			M	1	„:16R.“		
			Code	c	..16	M	1	„AMT“		
	D3	:19A:	Betrag			M	n	Gebühren, Spesen etc.		
			Tag			M	1	„:19A.“		
			Konstante			M	1	„.“		
			Qualifier	c	4	M	1	„ACRU“ = Betrag der Stückzinsen „EXEC“ = Provision des ausführenden Brokers „CHAR“ = Gebüh- ren/Spesen „LOCO“ = Maklerge- bühr/Courtage „COUN“ = Bundessteuer, Ländersteuer (ZAST, KEST) „DEAL“ = Betrag des Han- delsgeschäftes „ISDI“ = Bonifikation „LEVY“ = Steuer auf Zah-		

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen
								lung „LOCL“ = Lokale Steuer (Solidaritätszuschlag) „MACO“ = Clearing- und/oder Umschreibungs- gebühr „MARG“ = Betrag der Marge „ORGV“ = Ursprünglicher Nennwert „POST“ = Porto „REGF“ = XETRA-Gebühr „SHIP“ = Fracht „SPCN“ = Provision „STAM“ = Stempelsteuer (bei ausld. Wertpapieren) „STEX“ = Börsenumsatz- steuer „TRAN“ = Übertragungs- steuer „TRAX“ = Transaktions- steuer „VATA“ = Mehrwertsteuer „WITH“ = Quellensteuer „OTHR“ = Sonstige (Li- mitgebühr, Limitverwal- tungsgebühr, Gebühren für Änderun- gen/Streichungen) „RESU“ = Betrag der sich aus der Währungsum- rechnung ergibt (für alle Beträge außer OCMT) „OCMT“ = Abrechnungs- betrag (Feld C:19A:) um- gerechnet von/in Euro
			Konstante			M	1	„/“
			Vorzeichen	a	1	K	1	„N“ (nur wenn der Betrag negativ ist)
			Währungscode	a	3	M	1	ISO 4217-Code
			Betrag	d	..15	M	1	
	D3	:98A:	Wertstellungsdatum			K	1	
			Tag			M	1	„:98A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„VALU“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
	D3	:92B:	Wechselkurs			K	1	
			Tag			M	1	„:92B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„EXCH“

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 144	Län- ge	Sta- tus 145	An- zahl	Inhalt/Bemerkungen
D	D3		Konstante			M	1	„/“
			Erste Währung	a	3	M	1	ISO 4217-Code
			Konstante			M	1	„/“
			Zweite Währung	a	3	M	1	ISO 4217-Code
			Konstante			M	1	„/“
			Kurs/Satz	d	..15	M	1	
		:16S:	Blockende			M	1	
			Tag			M	1	„:16S:“
			Code	c	..16	M	1	„AMT“
		:16S:	Blockende			M	1	
			Tag			M	1	„:16S:“
			Code	c	..16	M	1	„SETDET“

• Häufig verwendete Abrechnungspositionen und ihre Zuordnung zu SWIFT-Feldern

Position der Abrechnung	Folge	Tag	Qualifier
Abrechnungs-(End-)betrag in Abrechnungswährung (inkl. Währungskennzeichen)	C	:19A:	SETT
Abrechnungs-(End-)betrag umgerechnet von/in Euro (inkl. Währungskennzeichen)	D3	:19A:	OCMT
Abrechnungsdatum	C	:98C:	SETT
Börsenplatz/Ausführungsort	C	:94B:	TRAD
Courtage/Maklergebühr (inkl. Währungskennzeichen)	D3	:19A:	LOCO
Depotnummer	C1	:97A:	SAFE
Devisen-/Wechselkurs	D3	:92B:	EXCH
Freitextliche Erläuterungen (Depotart, Verwahrart, Depot-schlüssel)	C2	:70E:	FIAN
Geld-/Verrechnungskonto	C1	:97A:	CASH
Handelsdatum	C	:98a:	TRAD
Kapitalertragssteuer/Zinsabschlagsteuer	D3	:19A:	COUN
Kennzeichen, ob Kauf oder Verkauf	C	:22H:	BUSE
Kurs/Preis	C	:90a:	DEAL
Kurswert in Abrechnungswährung	D3	:19A:	RESU
Kurswert in Handelswährung	D3	:19A:	DEAL
Kurszusatz	C	:22F:	TTCO
Nennwert	C	:36B:	CONF
Provision (inkl. Währungskennzeichen)	D3	:19A:	SPCN
Solidaritätszuschlag	D3	:19A:	LOCL
Spesen (inkl. Währungskennzeichen)	D3	:19A:	CHAR
Stückzahl	C	:36B:	CONF
Währung des Nennwertes	C2	:11A:	DENO
Wertpapierbezeichnung	C	:35B:	
Wertpapierkennnummer bzw. ISIN	C	:35B:	
Wertstellungsdatum	D3	:98A:	VALU
Zinsbetrag/Stückzinsen (inkl. Währungskennzeichen)	D3	:19A:	ACRU
Zinsdatum	C2	:98A:	COUP
Zinsmethode bzw. Kennzeichen, ob Berechnung abwei-	C2	:22F:	MICO

Position der Abrechnung	Folge	Tag	Qualifier
chend von deutscher Zinsmethode			
Zinssatz	C2	:92A:	INTR
Zinstage	C	:99A:	DAAC

- Beispiel**

Kauf von 50 Stammaktien der Mustermann AG zum Kurs von 52,70 Euro in Frankfurt/Main, Girosammelverwahrung. Abrechnungswährung ist Euro, ausgewiesen wird auch der entsprechende Endbetrag in DM.

Folge	Sub-folge	Beispiel
A		:16R:GENL :20C::SEME//NONREF :23G:NEWM :98C::PREP//19990305122030 :22F::TRTR//TRAD
	A1	:16R:LINK :20C::RELA//0000000000000000 :16S:LINK
		:16S:GENL
C		:16R:CONFDET :98C::TRAD//19990302112030 :98C::SETT//19990303112030 :90B::DEAL//ACTU/EUR52,7 :94B::TRAD//EXCH/XFRA :19A::SETT//NEUR2666,49 :22H::BUSE//BUYI :22F::PRIC//NET1 :22H::PAYM//APMT
	C1	:16R:CONFPTY :95Q::INVE//10020030 :97A::SAFE//10020030/1234567 :97A::CASH//10020030/987654321 :16S:CONFPTY
		:36B::CONF//UNIT/50,

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub-folge	Beispiel
		:35B:ISIN DE0123456789 /DE/123456 Mustermann AG, Stammaktien
	C2	:16R:FIA :22F::FORM//BEAR :22F::PREF//ORDN :16S:FIA
		:16S:CONFDET
D		:16R:SETDET :22F::SETR//TRAD :17B::STAN//N
	D3	:16R:AMT :19A::DEAL//NEUR2635, :19A::SPCN//NEUR26,35 :19A::LOCO//NEUR2,64 :19A::MACO//NEUR2,5 :19A::OCMT//NDEM5215,2 :98A::VALU//19990305 :92B::EXCH//EUR/DEM/1,95583 :16S:AMT
		:16S:SETDET -

Verkauf von 10.000 Australische Dollar „Anleihe Staat Australien, 6,25%“ zum Kurs von 105% in London; Abrechnungswährung ist Euro.

Folge	Sub-folge	Beispiel
A		:16R:GENL :20C::SEME//NONREF :23G:NEWM :98C::PREP//19990629153045 :22F::TRTR//TRAD

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub-folge	Beispiel
	A1	:16R:LINK :20C::RELA//000000000000000000 :16S:LINK
		:16S:GENL
C		:16R:CONFDET :98C::TRAD//19990625130510 :98C::SETT//19990628121212 :90A::DEAL//PRCT/105, :99A::DAAC//090 :94B::TRAD//EXCH/XISE :19A::SETT//EUR6296,9 :22H::BUSE//SELL :22F::PRIC//NET1 :22H::PAYM//APMT
	C1	:16R:CONFPTY :95Q::INVE//10020030 :97A::SAFE//10020030/1234567 :97A::CASH//10020030/987654321 :16S:CONFPTY
		:36B::CONF//FAMT/10000, :35B:ISIN AU9876543210 Australian Domestic Bonds 1993 (2003) SER. 10
	C2	:16R:FIA :22F::MICO//A001 :22F::PFRE//ANNU :11A::DENO//AUD :98A::COUP//20000401 :98A::MATU//20030401 :92A::INTR//6,25

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Beispiel
		:13B::COUP//7 :16S:FIA
		:16S:CONFDET
D		:16R:SETDET :22F::SETR//TRAD :17B::STAN//N
	D3	:16R:AMT :19A::DEAL//AUD10500, :19A::RESU//EUR6294,65 :92B::EXCH//AUD/EUR/0,59949 :16S:AMT
	D3	:16R:AMT :19A::ACRU//AUD150, :19A::RESU//EUR89,92 :92B::EXCH//AUD/EUR/0,59949 :16S:AMT
	D3	:16R:AMT :19A::EXEC//NGBP15, :19A::RESU//NEUR22,22 :92B::EXCH//EUR/GBP/0,6751 :16S:AMT
	D3	:16R:AMT :19A::SPCN//NEUR62,95 :19A::MACO//NEUR2,5 :19A::OCMT//DEM12315,67 :98A::VALU//19990701 :92B::EXCH//EUR/DEM/1,95583 :16S:AMT
		:16S:SETDET -

3.3.3 MT 535 Depotaufstellung

„Statement of Holdings“; basiert auf SWIFT „Standards Release Guide“,
Stand: Oktober 1998

- **Übersicht** (ohne konstante Felder)

Folge	Sub- folge	Tag	Sta- tus <small>146</small>	Inhalt
A			M	Allgemeine Informationen
		:28E:	M	Seitennummer/Indikator für Fortsetzung
		:13A:	K	Nummer der Aufstellung
		:98a:	K	Datum (und Uhrzeit), zu der die Aufstellung erstellt wurde
		:98a:	M	Datum (und Uhrzeit), auf dem/der die Aufstellung basiert
		:97A:	M	Depotkonto
		:17B:	M	Kennzeichen, ob Bestände vorhanden
B			K	Finanzinstrument
		:35B:	M	Wertpapierkennung und -bezeichnung
		:90a:	K	Preis (aktueller Kurs)
		:94B:	K	Ort (Herkunft von Preis/Kurs in B:90a:)
		:98a:	K	Notierungsdatum (und -uhrzeit) von Preis/Kurs in B:90a:
		:93B:	M	Gesamtstückzahl bzw. Nominale der Depotposition
	B1		M	Untersaldo
		:93C:	M	Saldo (Stückzahl bzw. Nominale der Unterposition zu B:93B:)
		:94C:	K	Depotstelle (Lagerland)
		:70C:	K	Freier Text für Einzelheiten zum Untersaldo
		:99A:	K	Anzahl der aufgelaufenen Tage für die Zinsberechnung (nur bei Rentenpapieren)
		:19A:	K	Wert der Depotposition in Währung des Feldes C:19A:
		:19A:	K	Wert der Depotposition in Depotwährung
		:19A:	K	Betrag der Stückzinsen in Währung des Feldes C:19A:
		:19A:	K	Betrag der Stückzinsen in Depotwährung
		:92B:	K	Wechselkurs
		:70E:	K	Zusatzinformationen zur Depotposition
C			K	Zusätzliche Informationen
		:19A:	M	Gesamtwert der Depotbestände der Nachricht

¹⁴⁶ M = Pflichtfeld, K = Kannfeld

• Belegungsrichtlinien

Folge	Sub- folge	Tag	Name	For- mat 147	Län- ge	Sta- tus 148	An- zahl	Inhalt/Bemerkungen
A			Allgemeine Informationen			M	1	
A	:16R:		Blockanfang			M	1	
			Tag			M	1	„:16R.“
			Code	c	..16	M	1	„GENL“
	:28E:		Seitennummer/Indikator für Fortsetzung			M	1	
			Tag			M	1	„:28E.“
			Seitennummer	n	..5	M	1	
			Konstante			M	1	„/“
			Indikator für Fortsetzung	c	4	M	1	„LAST“ = Letzte Seite „MORE“ = Zwischenseite (es folgen noch Seiten) „ONLY“ = Einzige Seite
A	:13A:		Nummer der Aufstellung			K	1	
			Tag			M	1	„:13A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„STAT“
			Konstante			M	1	„/“
			Numerische ID	c	3	M	1	Eindeutige Nummer der Aufstellung Die Nummer ist mit füh- renden Nullen aufzufüllen
A	:20C:		Referenz des Senders			M	1	
			Tag			M	1	„:20C.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„SEME“
			Konstante			M	1	„/“
			Referenz	x	..16	M	1	„NONREF“
A	:23G:		Funktion der Nachricht			M	1	
			Tag			M	1	„:23G.“
			Funktion	c	4	M	1	„NEWM“
A	:98a:		Erstellungsdatum			K	1	
			Option A:					
			Tag			M	1	„:98A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PREP“
			Konstante			M	1	„/“

¹⁴⁷ a = alpha (erlaubt sind „A“-„Z“), c = character (erlaubt sind „A“-„Z“ und „0“-„9“), d = dezimal (Fließkommazahl, der Vorkommaanteil muss wenigstens ein Zeichen enthalten, ein Dezimalkomma ist Pflicht und in der maximalen Länge enthalten), n = numerisch (erlaubt sind die Ziffern 0-9), x = alphanummerisch (erlaubt sind alle Zeichen aus dem SWIFT-Zeichensatz)

¹⁴⁸ M = Pflichtfeld, K = Kannfeld

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 147	Län- ge	Sta- tus 148	An- zahl	Inhalt/Bemerkungen
A			Datum	n	8	M	1	JJJJMMTT
			Option C:					
			Tag			M	1	„98C.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PREP“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Uhrzeit	n	6	M	1	hhmmss
		:98a:	Datum der Aufstellung			M	1	
			Option A:					
			Tag			M	1	„98A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„STAT“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Option C:					
			Tag			M	1	„98C.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„STAT“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Uhrzeit	n	6	M	1	hhmmss
A	:22F:		Art der Aufstellung			M	1	
			Tag			M	1	„22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„STTY“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„CUST“
A	:97A:		Depotkonto			M	1	
			Tag			M	1	„97A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„SAFE“
			Konstante			M	1	„/“
			Konto	x	..35	M	1	BLZ gefolgt von „/“ und der Kontonummer
A	:17B:		Merkmal für Aktivität			M	1	
			Tag			M	1	„17B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„ACTI“
			Konstante			M	1	„/“
			Merkmal	a	1	M	1	„Y“, wenn Depotbestände vorhanden (dann ist Folge B Pflicht) „N“, wenn keine Depotbestände vorhanden (dann muss Folge B ausgelassen werden)
A	:16S:		Blockende			M	1	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 147	Län- ge	Sta- tus 148	An- zahl	Inhalt/Bemerkungen
			Tag			M	1	„:16S.“
			Code	c	..16	M	1	„GENL.“
B			Finanzinstrument			K	n	Pro Gattung muss mindestens eine B-Sequenz eingestellt werden. Nach individuellen Kriterien können pro Gattung auch mehrere B-Sequenzen gebildet werden (z.B. für gesperrte und nicht gesperrte Bestände oder unterschiedliche Depot-schlüssel). ¹⁴⁹ Wenn keine Depotbestände vorhanden, muss Feld A:17B: mit „N“ belegt sein
B		:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R.“
			Code	c	..16	M	1	„FIN“
B		:35B:	Kennung des Finanz-instruments			M	1	Es muss entweder die ISIN oder die WKN oder beide angegeben werden.
			Tag			M	1	„:35B.“
			Konstante			K	1	„ISIN“ (nur wenn ISIN angegeben wird)
			Konstante			K	1	„ „ (Leerzeichen, nur wenn ISIN angegeben wird)
			ISIN-Kennung	x	..12	M	1	Wird keine ISIN verwendet, so ist „/DE/“ gefolgt von der deutschen Wert-papierkennnummer (WKN) anzugeben.
			Konstante			M	1	<CR><LF>
			Freier Text	x	..35	M	1..4	Wertpapierbezeichnung Falls ISIN und WKN ge-meinsam angegeben wer-den, ist die WKN in die erste Zeile und die Be-zeichnung in die Zeilen 2-4 einzustellen. Die Zeilen werden mit <CR><LF> getrennt.
B		:90a:	Preis			K	1	
			Option A:					falls der Preis ein Pro-

¹⁴⁹



Das Kundenprodukt kann beispielsweise als Kurzübersicht jeweils die Gattungen der B-Folge und als detaillierte Information auf Anforderung die zugehörigen B1-Folgen anzeigen.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 147	Län- ge	Sta- tus 148	An- zahl	Inhalt/Bemerkungen
B			zentsatz ist					
			Tag			M	1	„.90A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„MRKT“ = Marktpreis (z.B. aktueller Börsenkurs) „INDC“ = Hinweispreis (rechnerischer bzw. ermittelter Preis)
			Konstante			M	1	„/“
			Art der Prozentrechnung	c	4	M	1	„PRCT“
			Konstante			M	1	„/“
			Preis	d	..15	M	1	
			Option B: falls der Preis ein Betrag ist					
			Tag			M	1	„.90B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„MRKT“ = Marktpreis (z.B. Börsenkurs) „INDC“ = Hinweispreis (rechnerischer bzw. ermittelter Preis)
			Konstante			M	1	„/“
			Betrag Typ	c	4	M	1	„ACTU“
			Konstante			M	1	„/“
			Währung	a	3	M	1	ISO 4217-Währungscode
			Preis	d	..15	M	1	Die Anzahl der Nachkommastellen wird nicht gegen die Währung geprüft.
	:94B:		Ort (Herkunft von Preis/Kurs)			K	1	
			Tag			M	1	„.94B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PRIC“
			Konstante			M	1	„/“
			Ort	c	4	M	1	„LMAR“ = Lokale Börse „THEO“ = Theoretischer Wert, der auf der Marktrendite basiert „VEND“ = Verkäufer als Quelle
			Konstante			K	1	„/“ (nur, wenn Freier Text belegt)
			Freier Text	x	..30	K	1	Bei „LMAR“ kann hier der Name der Börse als MIC angegeben werden.
B	:98a:		Notierungsdatum von Preis/Kurs			K	1	
			Option A:					
			Tag			M	1	„.98A.“
			Konstante			M	1	„.“

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 147	Län- ge	Sta- tus 148	An- zahl	Inhalt/Bemerkungen
B			Qualifier	c	4	M	1	„PRIC“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Option C:					
			Tag			M	1	„:98C.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PRIC“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Uhrzeit	n	6	M	1	hhmmss
		:93B:	Gesamtsaldo			M	1	Stückzahl, ausgedrückt als Zahl oder Nennbetrag Die Stückzahl muss der Summe der Untersalden aus Feld B1:93C: entspre- chen
			Tag			M	1	„:93B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„AGGR“
			Konstante			M	1	„/“
			Stückzahl Typ	c	4	M	1	„FAMT“ = Die Stückzahl wird als Nennbetrag aus- gedrückt „UNIT“ = Die Stückzahl wird als Zahl (Zähler) aus- gedrückt
			Konstante	c	1	M	1	„/“
			Vorzeichen	a	..1	K	1	„N“ (nur wenn der Saldo negativ ist)
			Saldo	d	..15	M	1	Bei Nennbeträgen wird die Währung durch die „De- potwährung“ in Feld B:70E: bestimmt
	B1		Untersaldo			M	1..n	Jede Position der B-Folge ist mindestens einmal als B1-Folge zu wiederholen. Existieren zu einer B-Fol- ge mehrere Untersalden (z.B. gesperrt und nicht gesperrt), so ist für jede dieser Positionen eine B1- Folge einzustellen (s. Bei- spiel)
			Blockanfang			M	1	
			Tag			M	1	„:16R.“
	B1	:16R:	Code	c	..16	M	1	„SUBBAL“
			Saldo			M	1	Stückzahl, ausgedrückt als Zahl oder Nennbetrag
			Tag			M	1	„:93C.“
			Konstante			M	1	„.“
	B1	:93C:	Qualifier	c	4	M	1	„BLOK“ = Blockiert

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 147	Län- ge	Sta- tus 148	An- zahl	Inhalt/Bemerkungen
								„BORR“ = Geliehen „COLI“ = Sicherheit in „COLO“ = Sicherheit aus „LOAN“ = Ausgeliehen „NOMI“ = Im Namen eines Treuhänders „PECA“ = Schwebende Corporate Action „PEND“ = Schwebende Lieferung „PENR“ = Schwebender Eingang „REGO“ = Herausgege- ben zur Registrierung „RSTR“ = Eingeschränkt „SPOS“ = Außerbörsliche Position „TAVI“ = Insgesamt ver- fügbar „TRAN“ = In Übertragung Es ist darauf zu achten, dass diese Information nicht im Widerspruch zur Angabe im Feld „Saldo Code“ steht.
			Konstante			M	1	„/“
			Stückzahl Typ	c	4	M	1	„FAMT“ = Die Stückzahl wird als Nennbetrag aus- gedrückt „UNIT“ = Die Stückzahl wird als Zahl (Zähler) aus- gedrückt
			Konstante			M	1	„/“
			Saldo Code	c	4	M	1	„AVAI“ = Verfügbar (nicht gesperrt) „NAVL“ = Nicht verfügbar (gesperrt) Das Feld gibt an, ob das Papier für einen Verkauf zur Verfügung steht.
			Konstante			M	1	„/“
			Vorzeichen	a	..1	K	1	„N“ (nur wenn der Saldo negativ ist)
			Saldo	d	..15	M	1	
	B1	:94C:	Depotstelle			K	1	Lagerland
			Tag			M	1	„:94C:“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„SAFE“
			Konstante			M	1	„/“
			Land	a	2	M	1	ISO 3166-Ländercode
	B1	:70C:	Freier Text für Einzelhei- ten zum Untersaldo			K	1	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 147	Län- ge	Sta- tus 148	An- zahl	Inhalt/Bemerkungen
B	B1		Tag			M	1	„:70C:“
			Konstante			M	1	„:“
			Qualifier	c	4	M	1	„SUBB“
			Konstante			M	1	„/“
			Freier Text	x	..35	M	1..4	gemäß strukturierter Be- legung
		:16S:	Blockende			M	1	
			Tag			M	1	„:16S:“
			Code	c	..16	M	1	„SUBBAL“
		:99A:	Anzahl der aufgelaufenen Tage			K	1	
			Tag			M	1	„:99A:“
			Konstante			M	1	„:“
			Qualifier	c	4	M	1	„DAAC“
			Konstante			M	1	„/“
			Vorzeichen	a	..1	K	1	„N“ (nur wenn die Anzahl der Tage negativ ist)
			Nummer	n	3	M	1	Anzahl Tage (ggf. mit füh- renden Nullen auffüllen)
	B	:19A:	Depotwert			K	1	Kurswert zum Gesamtsal- do aus B:93B: in gleicher Währung wie C:19A:
			Tag			M	1	„:19A:“
			Konstante			M	1	„:“
			Qualifier	c	4	M	1	„HOLD“
			Konstante			M	1	„/“
			Vorzeichen	a	..1	K	1	„N“ (nur wenn der Betrag negativ ist)
			Währung	a	3	M	1	ISO 4217-Code
			Betrag	d	..15	M	1	
	B	:19A:	Depotwert			K	1	Kurswert zum Gesamtsal- do aus B:93B: (falls ab- weichend von Währung in C:19A:) a) bei prozentnotierten Papieren in Depotwäh- rung b) bei stücknotierten Pa- piere in der Währung des Preises in B:90B:
			Tag			M	1	„:19A:“
			Konstante			M	1	„:“
			Qualifier	c	4	M	1	„HOLD“
			Konstante			M	1	„/“
			Vorzeichen	a	..1	K	1	„N“ (nur wenn der Betrag negativ ist)
			Währung	a	3	M	1	ISO 4217-Code
			Betrag	d	..15	M	1	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 147	Län- ge	Sta- tus 148	An- zahl	Inhalt/Bemerkungen
B		:19A:	Betrag der Stückzinsen			K	1	Stückzinsbetrag zum Ge- samtaldo aus B:93B: in gleicher Währung wie C:19A:
			Tag			M	1	„:19A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„ACRU“
			Konstante			M	1	„/“
			Vorzeichen	a	..1	K	1	„N“ (nur wenn der Betrag negativ ist)
			Währung	a	3	M	1	ISO 4217-Code
			Betrag	d	..15	M	1	
B		:19A:	Betrag der Stückzinsen			K	1	Stückzinsbetrag zum Ge- samtaldo aus B:93B: in Depotwährung (falls ab- weichend von Währung in C:19A:)
			Tag			M	1	„:19A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„ACRU“
			Konstante			M	1	„/“
			Vorzeichen	a	..1	K	1	„N“ (nur wenn der Betrag negativ ist)
			Währung	a	3	M	1	ISO 4217-Code
			Betrag	d	..15	M	1	
B		:92B:	Wechselkurs			K	1	Es kann bspw. der Wech- selkurs zwischen den beiden Depotwert- oder Stückzinssbetragswährun- gen (B:19A:) angegeben werden.
			Tag			M	1	„:92B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„EXCH“
			Konstante			M	1	„/“
			Erste Währung	a	3	M	1	ISO 4217-Code
			Konstante			M	1	„/“
			Zweite Währung	a	3	M	1	ISO 4217-Code
			Konstante			M	1	„/“
			Kurs/Satz	d	..15	M	1	
B		:70E:	Freier Text zu Depotbe- ständen			K	1	
			Tag			M	1	„:70E.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„HOLD“
			Konstante			M	1	„/“
			Freier Text	x	..35	M	1..4	gemäß strukturierter Be- legung
B		:16S:	Blockende			M	1	
			Tag			M	1	„:16S.“

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 147	Län- ge	Sta- tus 148	An- zahl	Inhalt/Bemerkungen
			Code	c	..16	M	1	„FIN“
C			Zusätzliche Informationen			K	1	Bei einem unbewerteten Depotbestand wird Folge C nicht gesendet.
C		:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R:“
			Code	c	..16	M	1	„ADDINFO“
		:19A:	Gesamtwert der Depotbestände der Nachricht			M	1	Summe der Beträge aus B:19A: (d.h. sowohl Kurswerte als auch Stückzinsen)
			Tag			M	1	„:19A:“
			Konstante			M	1	„-“
			Qualifier	c	4	M	1	„HOLP“
			Konstante			M	1	„/“
			Vorzeichen	a	..1	K	1	„N“ (nur wenn der Betrag negativ ist)
			Währung	a	3	M	1	ISO 4217-Code
C			Betrag	d	..15	M	1	
		:16S:	Blockende			M	1	
			Tag			M	1	„:16S:“
			Code	c	..16	M	1	„ADDINFO“

- Beispiel**

Bei der ersten Depotposition (Mustermann AG Stammaktien) liegt ein Bestand von 100 Stück vor. Die zweite Position (Mustermann AG Vorzugsaktien) setzt sich aus einem Guthaben von 130 Stück und einem schwebenden Abgang von 30 Stück zu einem Saldo von 100 Stück zusammen. Bei der dritten Position (Australian Domestic Bonds) ist im Gesamtsaldo von 10.000 Australischen Dollar ein Bestand von 2.500 Dollar als gesperrt gekennzeichnet.

Folge	Sub- folge	Beispiel
A		:16R:GENL :28E:1/ONLY :13A::STAT//004 :20C::SEME//NONREF :23G:NEWM :98C::PREP//19990530120538 :98A::STAT//19990529 :22F::STTY//CUST

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Beispiel
		:97A::SAFE//10020030/1234567 :17B::ACTI//Y :16S:GENL
B		:16R:FIN :35B:ISIN DE0123456789 /DE/123456 Mustermann AG, Stammaktien :90B::MRKT//ACTU/EUR52,7 :94B::PRIC//LMAR/XFRA :98A::PRIC//19990529 :93B::AGGR//UNIT/100,
	B1	:16R:SUBBAL :93C::TAVI//UNIT/AVAI/100, :94C::SAFE//DE :70C::SUBB//12345678901234567890 1 :16S:SUBBAL
		:19A::HOLD//EUR5270, :70E::HOLD//STK+511+00081+DE+19990815 68,5+EUR :16S:FIN
B		:16R:FIN :35B:ISIN DE0123456790 /DE/123457

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Beispiel
		<p>Mustermann AG, Vorzugsaktien</p> <p>:90B::MRKT//ACTU/EUR54,6</p> <p>:94B::PRIC//LMAR/XFRA</p> <p>:98A::PRIC//19990529</p> <p>:93B::AGGR//UNIT/100,</p>
	B1	<p>:16R:SUBBAL</p> <p>:93C::TAVI//UNIT/AVAI/130,</p> <p>:94C::SAFE//DE</p> <p>:70C::SUBB//123456799123456799</p> <p>1</p> <p>:16S:SUBBAL</p>
	B1	<p>:16R:SUBBAL</p> <p>:93C::PEND//UNIT/NAVL/N30,</p> <p>:94C::SAFE//DE</p> <p>:70C::SUBB//123456799123456799</p> <p>1</p> <p>:16S:SUBBAL</p>
		<p>:19A::HOLD//EUR5460,</p> <p>:70E::HOLD//STK+512+00081+DE+19981013</p> <p>42,75+EUR</p> <p>:16S:FIN</p>
B		<p>:16R:FIN</p> <p>:35B:ISIN AU9876543210</p> <p>Australian Domestic Bonds</p>

Folge	Sub- folge	Beispiel
		1993 (2003) Ser. 10 :90A::MRKT//PRCT/105, :94B::PRIC//LMAR/XASX :98A::PRIC//19990528 :93B::AGGR//FAMT/10000,
	B1	:16R:SUBBAL :93C::TAVI//FAMT/AVAI/7500, :94C::SAFE//AU :70C::SUBB//98765432109876543210 4+Sydney :16S:SUBBAL
	B1	:16R:SUBBAL :93C::BLOK//FAMT/NAVL/2500, :94C::SAFE//AU :70C::SUBB//98765432109876543210 4+Sydney+20021231 :16S:SUBBAL
		:99A::DAAC//004 :19A::HOLD//EUR6294,65 :19A::HOLD//AUD10500, :19A::ACRU//EUR1,72 :19A::ACRU//AUD2,87 :92B::EXCH//AUD/EUR/0,59949 :70E::HOLD//AUD+525+00611+AU+19990315+200312

Folge	Sub-folge	Beispiel
		31 99,75++6,25 :16S:FIN
C		:16R:ADDINFO :19A::HOLP//EUR17026,37 :16S:ADDINFO -

• Strukturierte Belegung des Feldes :70E:

Jede Zeile beginnt mit einer Ziffer, die die Zeilennummer angibt. Die Felder sind jeweils durch „+“ zu trennen. Wird ein Feld nicht belegt, so ist das Auslassen durch das Setzen des Trennzeichens zu kennzeichnen. Vor dem ersten und hinter dem letzten Feld wird kein Trennzeichen eingefügt. Nicht belegte Felder am Ende einer Zeile können inklusive des Trennzeichens entfallen. Die Zeilen werden jeweils mit <CR><LF> getrennt. Nicht belegte Zeilen am Ende des S.W.I.F.T.-Freitextfeldes können entfallen.

Die Zeilen 3 und 4 sind nur bei Terminkontrakten zu belegen.

Nr.	Name	Format 150	Länge	Status 151	Anzahl	Bemerkungen
Zeile 1						
1	Zeilennummer	n	1	M	1	„1“
2	Depotwährung	a	3	K	1	„STK“ = stücknotierte Wertpapiere „KON“ = Kontrakte oder ISO-Währungscode der Gattungswährung bei prozentnotierten Wertpapieren
3	Wertpapierart	n	3	K	1	gemäß WM GD 195
4	Branchenschlüssel	n	5	K	1	gemäß WM GD 200
5	Land des Emittenten	a	2	K	1	gemäß ISO 3166-Ländercode
6	Kaufdatum	n	8	K	1	JJJJMMTT

¹⁵⁰ a = alpha (erlaubt sind „A“-„Z“), c = character (erlaubt sind „A“-„Z“ und „0“-„9“), d = dezimal (Fließkommazahl, der Vorkommaanteil muss wenigstens ein Zeichen enthalten, ein Dezimalkomma ist Pflicht und in der maximalen Länge enthalten), n = numerisch (erlaubt sind die Ziffern 0-9), x = alphanummerisch (erlaubt sind alle Zeichen aus dem SWIFT-Zeichensatz)

¹⁵¹ M = Pflichtfeld, K = Kannfeld

DFÜ – Abkommen

Anlage 3 (Datenformate)

Nr.	Name	Format 150	Länge	Status 151	Anzahl	Bemerkungen
7	Fälligkeitsdatum	n	8	K	1	JJJJMMTT (z.B. bei Rentenpapieren oder Optionsscheinen)
Zeile 2						
8	Zeilennummer	n	1	M	1	„2“
9	Einstandspreis/-kurs, Betrag	d	..15	K	1	ggf. Durchschnittswert
10	Einstandspreis/-kurs, Währung	a	3	K	1	ISO 4217-Währungscode (nur, wenn auch Betrag belegt ist) Wenn im Betragsfeld eine Prozentangabe erfolgt, wird das Währungsfeld nicht belegt.
11	Zinssatz	d	..15	K	1	als Prozentangabe bei verzinslichen Papieren
Zeile 3						
12	Zeilennummer	n	1	M	1	„3“
13	Schlüssel des Terminkontraktes	a	1	K	1	„C“ = Call „P“ = Put „F“ = Future
14	Verfalldatum des Terminkontraktes	n	6	K	1	JJJJMM
15	Version des Terminkontraktes	n	1	K	1	z.B. 0/1/2/3
16	Unit/Kontraktgröße des Terminkontraktes	n	..8	K	1	
17	Symbol	a	..4	K	1	Kürzel (z.B. „FDAX“, „BMW“)
18	WKN des Underlying	n	6	K	1	
Zeile 4						
19	Zeilennummer	n	1	M	1	„4“
20	ISIN des Underlying	x	12	K	1	
21	Basispreis des Terminkontraktes, Betrag	d	..15	K	1	Betrag
22	Basispreis des Terminkontraktes, Währung	a	3	K	1	ISO 4217-Währungscode (nur, wenn auch Betrag belegt ist)

• Beispiel

bei Aktien:

1STK+511+00081+DE+19990815
268,5+EUR

bei Renten:

1EUR+141+00024+DE+19990930+20051001
2100,25++5,25

bei Optionen:

1KON+857+00170+US+19991028+20001015
21247,75+EUR

3C+200010+1+500+BMW+519000

4DE0005190003+1000,+EUR

- **Strukturierte Belegung des Feldes :70C:**
Es gelten dieselben Regeln wie für das Feld :70E: (s.o.).

Nr.	Name	Format 152	Länge	Status 153	Anzahl	Bemerkungen
Zeile 1						
1	Zeilennummer	n	1	M	1	„1“
2	Depotschlüssel	x	..34	K	1	institutsindividuell zu belegen Der Depotschlüssel dient u.a. im Feld B2:70E: des MT 502 zur Identifizierung der Depotposition bei Verkäufen.
Zeile 2						
3	Zeilennummer	n	1	M	1	„2“
4	Verwahrart	n	1	K	1	1 = Girosammelverwahrung 2 = Streifbandverwahrung 3 = Haussammelverwahrung 4 = Wertpapierrechnung 9 = Sonstige
5	Lagerstelle	x	..15	K	1	Freitext
6	Sperre bis	n	8	K	1	JJJJMMTT
Zeile 3						
7	Zeilennummer	n	1	M	1	„3“
8	Sperrvermerke/Zusatzvermerke der Bank	x	..34	K	1	Freitext
Zeile 4						
9	Zeilennummer	n	1	M	1	„4“
10	Sperrvermerke/Zusatzvermerke der Bank	x	..34	K	1	Freitext

- **Beispiel**

112345678901234567890

21+London+20021231

3Verpfaendet fuer Darlehen Nr 6020

¹⁵² a = alpha (erlaubt sind „A“-„Z“), c = character (erlaubt sind „A“-„Z“ und „0“-„9“), d = dezimal (Fließkommazahl, der Vorkommaanteil muss wenigstens ein Zeichen enthalten, ein Dezimalkomma ist Pflicht und in der maximalen Länge enthalten), n = numerisch (erlaubt sind die Ziffern 0-9), x = alphanumerisch (erlaubt sind alle Zeichen aus dem SWIFT-Zeichensatz)

¹⁵³ M = Pflichtfeld, K = Kannfeld

3.3.4 MT 536 Depotumsatzinformation

„Statement of Transactions“; basiert auf SWIFT „Standards Release Guide“, Stand: Oktober 1998

- **Übersicht** (ohne konstante Felder)

Folge	Sub-folge	Tag	Sta-tus ¹⁵⁴	Inhalt
A			M	Allgemeine Informationen
		:28E:	M	Seitennummer/Indikator für Fortsetzung
		:13A:	K	Nummer der Aufstellung
		:98a:	K	Datum (und Uhrzeit), zu der die Aufstellung erstellt wurde
		:69a:	M	Periode für die Aufstellung
		:97A:	M	Depotkonto
		:17B:	M	Kennzeichen, ob Umsätze stattgefunden haben
B			K	Finanzinstrument
		:35B:	M	Wertpapierkennung und -bezeichnung
		:90a:	K	Preis/Abrechnungskurs
		:94B:	K	Ort (Herkunft von Preis/Kurs)
		:98a:	K	Notierungsdatum (und -uhrzeit) von Preis/Kurs
		:93B:	K	Bestand vor und nach der Transaktion
	B1		M	Transaktion
	B1b		K	Einzelheiten der Transaktion
		:36B:	M	Gebuchte Stückzahl
		:99A:	K	Anzahl der aufgelaufenen Tage für die Zinsberechnung (nur bei Rentenpapieren)
		:19A:	K	Gebuchter Betrag/Kurswert
		:19A:	K	Betrag der Stückzinsen
		:22F:	M	Indikator für die Transaktion
		:22H:	M	Indikator für Eingang/Lieferung
		:98a:	M	Effektives Abrechnungsdatum (Schlusstag)
		:98a:	K	Valutadatum
		:25D:	K	Status einer Bewegung (Stornokennzeichen)
		:70E:	K	Freier Text zu Einzelheiten der Transaktion

¹⁵⁴ M = Pflichtfeld, K = Kannfeld

• Belegungsrichtlinien

Folge	Sub- folge	Tag	Name	For mat ¹⁵⁵	Län ge	Stat us ¹⁵⁶	An- zahl	Inhalt/Bemerkungen
A			Allgemeine Informationen			M	1	
A		:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R:“
			Code	c	..16	M	1	„GENL“
A		:28E:	Seitennummer/Indikator für Fortsetzung			M	1	
			Tag			M	1	„:28E:“
			Seitennummer	n	..5	M	1	
			Konstante			M	1	„/“
			Indikator für Fortsetzung	c	4	M	1	„LAST“ = Letzte Seite „MORE“ = Zwischenseite (es folgen noch Seiten) „ONLY“ = Einzige Seite
A		:13A:	Nummer der Aufstellung			K	1	
			Tag			M	1	„:13A:“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„STAT“
			Konstante			M	1	„/“
			Numerische ID	c	3	M	1	Eindeutige Nummer der Aufstellung Die Nummer ist mit füh- renden Nullen aufzufüllen
A		:20C:	Referenz des Senders			M	1	
			Tag			M	1	„:20C:“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„SEME“
			Konstante			M	1	„/“
			Referenz	x	..16	M	1	„NONREF“
A		:23G:	Funktion der Nachricht			M	1	
			Tag			M	1	„:23G:“
			Funktion	c	4	M	1	„NEWM“
A		:98a:	Erstellungsdatum			K	1	
			Option A:					
			Tag			M	1	„:98A:“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PREP“
			Konstante			M	1	„/“

¹⁵⁵ a = alpha (erlaubt sind „A“-„Z“), c = character (erlaubt sind „A“-„Z“ und „0“-„9“), d = dezimal (Fließkommazahl, der Vorkommaanteil muss wenigstens ein Zeichen enthalten, ein Dezimalkomma ist Pflicht und in der maximalen Länge enthalten), n = numerisch (erlaubt sind die Ziffern 0-9), x = alphanummerisch (erlaubt sind alle Zeichen aus dem SWIFT-Zeichensatz)

¹⁵⁶ M = Pflichtfeld, K = Kannfeld

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 155	Län- ge	Stat- us 156	An- zahl	Inhalt/Bemerkungen		
A			Datum	n	8	M	1	JJJJMMTT		
			Option C:							
			Tag			M	1	„:98C.“		
			Konstante			M	1	„.“		
			Qualifier	c	4	M	1	„PREP“		
			Konstante			M	1	„/“		
			Datum	n	8	M	1	JJJJMMTT		
			Uhrzeit	n	6	M	1	hhmmss		
	A	:69a:		Periode für die Aufstellung			M	1		
				Option A:						
				Tag			M	1	„:69A.“	
				Konstante			M	1	„.“	
				Qualifier	c	4	M	1	„STAT“	
				Konstante			M	1	„/“	
				von Datum	n	8	M	1	JJJJMMTT	
				Konstante			M	1	„/“	
				bis Datum	n	8	M	1	JJJJMMTT	
				Option B:						
			Tag			M	1	„:69B.“		
			Konstante			M	1	„.“		
			Qualifier	c	4	M	1	„STAT“		
			Konstante			M	1	„/“		
			von Datum	n	8	M	1	JJJJMMTT		
			Uhrzeit	n	6	M	1	hhmmss		
A			:97A:		Depotkonto			M	1	
					Tag			M	1	„:97A.“
		Konstante				M	1	„.“		
		Qualifier		c	4	M	1	„SAFE“		
		Konstante				M	1	„/“		
		Konto		x	..35	M	1	BLZ gefolgt von „/“ und der Kontonummer		
	A	:17B:			Merkmal für Aktivität			M	1	
					Tag			M	1	„:17B.“
					Konstante			M	1	„.“
					Qualifier	c	4	M	1	„ACTI“
					Konstante			M	1	„/“
					Merkmal	a	1	M	1	„Y“, wenn Umsätze vor- handen (dann ist Folge B Pflicht) „N“, wenn keine Umsätze stattgefunden haben (dann muss Folge B aus- gelassen werden)
	A	:16S:			Blockende			M	1	
					Tag			M	1	„:16S.“

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 155	Län- ge	Stat- us 156	An- zahl	Inhalt/Bemerkungen
			Code	c	..16	M	1	„GENL“
B			Finanzinstrument			K	n	
B	:16R:	Blockanfang				M	1	
		Tag				M	1	„:16R:“
		Code	c	..16	M	1	„FIN“	
	:35B:	Kennung des Finanzin- struments				M	1	Es muss entweder die ISIN oder die WKN oder beide angegeben werden.
		Tag				M	1	„:35B:“
		Konstante				K	1	„ISIN“ (nur wenn ISIN angegeben wird)
		Konstante				K	1	„ „ (Leerzeichen, nur wenn ISIN angegeben wird)
		ISIN-Kennung	x	..12	M	1	Wird keine ISIN verwen- det, so ist „/DE/“ gefolgt von der deutschen Wert- papierkennnummer (WKN) anzugeben.	
		Konstante				M	1	<CR><LF>
		Freier Text	x	..35	M	1..4	Wertpapierbezeichnung Falls ISIN und WKN ge- meinsam angegeben werden, ist die WKN in die erste Zeile und die Bezeichnung in die Zeilen 2-4 einzustellen. Die Zeilen werden mit <CR><LF> getrennt.	
	B	:90a:	Preis				K	1
Option A:						falls der Preis ein Pro- zentsatz ist		
Tag						M	1	„:90A:“
Konstante						M	1	„.“
Qualifier			c	4	M	1	„MRKT“ = Marktpreis (z.B. Börsenkurs) "INDC" = Hinweispreis (rechnerischer bzw. ermit- telter Preis)	
Konstante						M	1	„/“
Art der Prozentrechnung			c	4	M	1	„PRCT“	
Konstante						M	1	„/“
Preis			d	..15	M	1		
Option B:						falls der Preis ein Betrag ist		
Tag						M	1	„:90B:“
Konstante						M	1	„.“
Qualifier	c	4	M	1	„MRKT“ = Marktpreis (z.B. Börsenkurs) "INDC" = Hinweispreis (rechnerischer bzw. ermit- telter Preis)			

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For mat 155	Län ge	Stat us 156	An- zahl	Inhalt/Bemerkungen
B			Konstante			M	1	„/“
			Betrag Typ	c	4	M	1	„ACTU“
			Konstante			M	1	„/“
			Währung	a	3	M	1	ISO 4217-Währungscode
			Preis	d	..15	M	1	Die Anzahl der Nachkom- mastellen wird nicht ge- gen die Währung geprüft.
	:94B:		Ort (Herkunft von Preis/ Kurs)			K	1	
			Tag			M	1	„:94B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PRIC“
			Konstante			M	1	„/“
			Ort	c	4	M	1	„LMAR“ = Lokale Börse „THEO“ = Theoretischer Wert, der auf der Markt- rendite basiert „VEND“ = Verkäufer als Quelle
			Konstante			K	1	„/“ (nur, wenn Freier Text belegt)
			Freier Text	x	..30	K	1	Bei „LMAR“ kann hier der Name der Börse als MIC angegeben werden.
	:98a:		Notierungsdatum von Preis/Kurs			K	1	
			Option A:					
			Tag			M	1	„:98A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PRIC“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Option C:					
			Tag			M	1	„:98C.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PRIC“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Uhrzeit	n	6	M	1	hhmmss
B	:93B:		Saldo			K	n	Stückzahl, ausgedrückt als Zahl oder Nennbetrag
			Tag			M	1	„:93B.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„FIOP“ = Erster Eröff- nungssaldo „INOP“ = Eröffnungssaldo als Zwischensaldo „FICL“ = Endgültiger Ab- schlussaldo „INCL“ = Abschlussaldo

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For mat 155	Län ge	Stat us 156	An- zahl	Inhalt/Bemerkungen
								als Zwischensaldo
			Konstante			M	1	„/“
			Stückzahl Typ	c	4	M	1	„FAMT“ = Die Stückzahl wird als Nennbetrag ausgedrückt „UNIT“ = Die Stückzahl wird als Zahl (Zähler) ausgedrückt
			Konstante			M	1	„/“
			Vorzeichen	a	..1	K	1	„N“ (nur wenn der Saldo negativ ist)
			Saldo	d	..15	M	1	
		B1	Transaktion			M	1	
		:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R:“
			Code	c	..16	M	1	„TRAN“
	B1a		Verbindungen			M	1	
		:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R:“
			Code	c	..16	M	1	„LINK“
	B1a	:20C:	Referenz des Senders			M	1	
			Tag			M	1	„:20C:“
			Konstante			M	1	„-“
			Qualifier	c	4	M	1	„RELA“
			Konstante			M	1	„/“
			Referenz	x	..16	M	1	„NONREF“
	B1a	:16S:	Blockende			M	1	
			Tag			M	1	„:16S:“
			Code	c	..16	M	1	„LINK“
	B1b		Einzelheiten der Transaktion			K	1	Angaben gemäß Abrechnung/Depotbuchung
	B1b	:16R:	Blockanfang			M	1	
			Tag			M	1	„:16R:“
			Code	c	..16	M	1	„TRANSDDET“
	B1b	:36B:	Gebuchte Stückzahl			M	1	
			Tag			M	1	„:36B:“
			Konstante			M	1	„-“
			Qualifier	c	4	M	1	„PSTA“
			Konstante			M	1	„/“
			Typ	c	4	M	1	„FAMT“ = Die Stückzahl wird als Nennbetrag ausgedrückt „UNIT“ = Die Stückzahl wird als Zahl (Zähler) ausgedrückt
			Konstante			M	1	„/“
			Stückzahl	d	..15	M	1	
	B1b	:99A:	Anzahl der aufgelaufenen Tage			K	1	z.B. Stückzinstage gemäß Abrechnung

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For mat 155	Län ge	Stat us 156	An- zahl	Inhalt/Bemerkungen
	B1b		Tag			M	1	„:99A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„DAAC“
			Konstante			M	1	„/“
			Vorzeichen	a	..1	K	1	„N“ (nur wenn die Anzahl der Tage negativ ist)
			Nummer	n	3	M	1	ggf. mit führenden Nullen auffüllen
		:19A:	Gebuchter Betrag			K	1	Kurswert
			Tag			M	1	„:19A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PSTA“
			Konstante			M	1	„/“
			Vorzeichen	a	..1	K	1	„N“ (nur wenn der Betrag negativ ist)
			Währung	a	3	M	1	ISO 4217-Code
			Betrag	d	..15	M	1	
		:19A:	Betrag der Stückzinsen			K	1	
			Tag			M	1	„:19A.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„ACRU“
			Konstante			M	1	„/“
			Vorzeichen	a	..1	K	1	„N“ (nur wenn der Betrag negativ ist)
			Währung	a	3	M	1	ISO 4217-Code
			Betrag	d	..15	M	1	
	B1b	:22F:	Indikator für die Transaktion			M	1	
			Tag			M	1	„:22F.“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„TRAN“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„BOLE“ = Aktivität im Zusammenhang mit Leihen/Verleihen „COLL“ = Aktivität im Zusammenhang mit Sicherheiten „CORP“ = Aktivität im Zusammenhang mit einer Corporate Action (z.B. Übertragung) „SETT“ = Aktivität im Zusammenhang mit Abrechnung und Clearing (i.d.R. bei Kauf und Verkauf)
		:22H:	Indikator für Eingang/Lieferung			M	1	
			Tag			M	1	„:22H.“
			Konstante			M	1	„.“

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For mat 155	Län ge	Stat us 156	An- zahl	Inhalt/Bemerkungen
	B1b		Qualifier	c	4	M	1	„REDE“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„DELI“ = Lieferung (Belastung) „RECE“ = Eingang (Gutschrift)
		:22H:	Indikator für Zahlungsweise			M	1	
			Tag			M	1	„:22H:“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„PAYM“
			Konstante			M	1	„/“
			Indikator	c	4	M	1	„FREE“
	B1b	:98a:	Effektives Abrechnungsdatum			M	1	Schlusstag
			Option A:					
			Tag			M	1	„:98A:“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„ESET“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Option C:					
			Tag			M	1	„:98C:“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„ESET“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Uhrzeit	n	6	M	1	hhmmss
	B1b	:98a:	Abrechnungsdatum			K	1	Valutadatum
			Option A:					
			Tag			M	1	„:98A:“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„SETT“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Option C:					
			Tag			M	1	„:98C:“
			Konstante			M	1	„.“
			Qualifier	c	4	M	1	„SETT“
			Konstante			M	1	„/“
			Datum	n	8	M	1	JJJJMMTT
			Uhrzeit	n	6	M	1	hhmmss
	B1b	:25D:	Status einer Bewegung			K	1	Feld wird nur gesendet, wenn Bewegung die Umkehrung einer vorherigen Bewegung ist (Stornokennzeichen)
			Tag			M	1	„:25D:“

Folge	Sub- folge	Tag	Name	For mat 155	Län ge	Stat us 156	An- zahl	Inhalt/Bemerkungen
B	B1b		Konstante			M	1	„“
			Qualifier	c	4	M	1	„MOVE“
			Konstante			M	1	„/“
			Status	c	4	M	1	„REVE“
		:70E:	Freier Text zu Einzelheiten der Transaktion			K	1	
			Tag			M	1	„:70E.“
			Konstante			M	1	„“
			Qualifier	c	4	M	1	„TRDE“
			Konstante			M	1	„/“
			Freier Text	x	..35	M	1..10	beliebige Informationen zum Umsatz (keine strukturierte Belegung wie im MT 535)
		:16S:	Blockende			M	1	
			Tag			M	1	„:16S.“
			Code	c	..16	M	1	„TRANSDT“
	B1	:16S:	Blockende			M	1	
			Tag			M	1	„:16S.“
			Code	c	..16	M	1	„TRAN“
		:16S:	Blockende			M	1	
			Tag			M	1	„:16S.“
			Code	c	..16	M	1	„FIN“

• Beispiel

Innerhalb des Berichtszeitraumes fanden drei Umsätze statt:

1. Kauf (Zugang) von 100 Stück Mustermann AG mit Schlusstag 15. Mai 1999
2. Verkauf (Abgang) von 70 Stück Mustermann AG mit Schlusstag 28. Mai 1999
3. Verkauf (Abgang) von 5.000 CAD 6,5 % DaimlerChrysler Lux. Fin. mit Schlusstag 21. Mai 1999

Folge	Sub- folge	Sub- folge	Beispiel
A			:16R:GENL :28E:1/ONLY :13A::STAT//005 :20C::SEME//NONREF :23G:NEWM

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Sub- folge	Beispiel
			:98A::PREP//19990530 :69A::STAT//19990501/19990529 :97A::SAFE//10020030/1234567 :17B::ACTI//Y :16S:GENL
	B		:16R:FIN :35B:ISIN DE0123456789 /DE/123456 Mustermann AG, Stammaktien :90B::MRKT//ACTU/EUR52,7 :94B::PRIC//LMAR/XFRA :98A::PRIC//19990515 :93B::FIOP//UNIT/200, :93B::FICL//UNIT/300,
		B1	:16R:TRAN
		B1a	:16R:LINK :20C::RELA//NONREF :16S:LINK
		B1b	:16R:TRANSDet :36B::PSTA//UNIT/100, :19A::PSTA//NEUR5270, :22F::TRAN//SETT :22H::REDE//RECE :22H::PAYM//FREE

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Sub- folge	Beispiel
			:98A::ESET//19990515 :98A::SETT//19990517 :16S:TRANSDET
			:16S:TRAN
			:16S:FIN
B			:16R:FIN :35B:ISIN DE0123456789 /DE/123456 Mustermann AG, Stammaktien :90B::MRKT//ACTU/EUR61,9 :94B::PRIC//LMAR/XFRA :98A::PRIC//19990528 :93B::FIOP//UNIT/300, :93B::FICL//UNIT/230,
	B1		:16R:TRAN
		B1a	:16R:LINK :20C::RELA//NONREF :16S:LINK
		B1b	:16R:TRANSDET :36B::PSTA//UNIT/70, :19A::PSTA//EUR4333, :22F::TRAN//SETT :22H::REDE//DELI :22H::PAYM//FREE

Folge	Sub- folge	Sub- folge	Beispiel
			:98A::ESET//19990528 :98A::SETT//19990530 :16S:TRANSDET
			:16S:TRAN
			:16S:FIN
B			:16R:FIN :35B:/DE/987654 DaimlerChrysler Lux. Fin. 1999 (2002) :90B::MRKT//PRCT/105, :94B::PRIC//LMAR/XLUX :98A::PRIC//19990521 :93B::FIOP//FAMT/5000,
	B1		:16R:TRAN
		B1a	:16R:LINK :20C::RELA//NONREF :16S:LINK
		B1b	:16R:TRANSDET :36B::PSTA//FAMT/5000, :99A::DAAC//003 :19A::PSTA//CAD5250, :19A::ACRU//CAD2,71 :22F::TRAN//SETT :22H::REDE//DELI

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Sub- folge	Beispiel
			:22H::PAYM//FREE
			:98A::ESET//19990521
			:98A::SETT//19990526
			:16S:TRANSDET
			:16S:TRAN
			:16S:FIN
			-

3.4 Akkreditivgeschäft

3.4.1 DTAEA Export-Akkreditiv-Avisierung und –änderung (Bank an Kunde)

Der Datensatz DTAEA kann – neben der üblichen Verwendung – auch zusätzlich zu Informationszwecken weiteren Empfängern bereit gestellt werden. In diesem Fall ist im Feld :A1: des Datenvorsatzes die Konstante „EAI“ zu verwenden und das Feld :M24: in der Akkreditivavisierung, der Akkreditivänderung beziehungsweise dem Freiformat zu belegen. Dieses bewirkt, dass die Nachricht im Verhältnis gegenüber Dritten – beispielsweise zu externen Dienstleistern – ausschließlich informatorischen Charakter besitzt und infolgedessen für die beteiligten Kreditinstitute keine Verpflichtung begründet.

Alle Felder inklusive Satzendeckennung werden mit <CR><LF> (X'0D0A') abgeschlossen.

Zugelassener Zeichencode ¹⁵⁷	Zeichen	Hexcode
Nummerische Zeichen	0 bis 9	X '30' - X '39'
Großbuchstaben	A bis Z	X '41' - X '5A'
<u>Sonderzeichen:</u>		
Leerzeichen	" "	X '20'
Punkt	"."	X '2E'
Komma	","	X '2C'
Trennstrich	"-"	X '2D'
Schrägstrich	"/"	X '2F'
Pluszeichen	"+"	X '2B'
Doppelpunkt	"."	X '3A'
Klammer auf	"("	X '28'
Klammer zu	")"	X '29'
Hochkomma	"'"	X '27'

Die Umlaute Ä, Ö; Ü sind wie AE, OE, UE und ß wie SS aufzuzeichnen.

Anzahl des Auftretens in logischer Datei	Element (jeweils mit Satzendeckennung)
1	Datenträgervorsatz EAB/EAI
0-n	Akkreditivavisierung 700, 710, 720 oder Akkreditivänderung 707
0-n	Freiformat 799
1	Datenträgnachsatz Z

¹⁵⁷ Codierung gemäß DIN 66003 (Ausgabe Juni 1974), Code Tabelle 2, Deutsche Referenz Version.

Datenträgervorsatz EAB/EAI

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁵⁸	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁵⁹	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:A1:	Kennzeichnung Vorsatz	an	3	F	P	Konstante „EAB“ oder Konstante „EAI“ für Kopie zur Information	
:A2:	Bankleitzahl oder SWIFT-BIC	an	11	V	P	Bankleitzahl oder SWIFT-BIC des absen- denden Kreditinstitutes	
:A3:	Kundennummer des Empfängers	an	23	V	P	Ordnungsnummer gemäß Vereinbarung mit dem sendenden Kreditinstitut (gegebenenfalls Kontonummer)	
:A4:	Empfängerdaten	an	4 x 35	V	K	Daten zum Feld :A3: Zeile 1 und 2: Name Zeile 3: Straße/Postfach Zeile 4: Ort	
:A5:	Dateimerkmal	an	8	F	K	Für mögliche Kundenrückfragen bezüglich der Datei: laufender Tag des Jahres (drei Stellen) Konstante „.“ Uhrzeit HHMM	
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

¹⁵⁸ an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁵⁹ P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Akkreditivavisierung 700, 710, 720

Feld-Nr.	Bezeichnung	Daten-format ¹⁶⁰	Länge in Bytes	variabel/fest	Kann/Pflicht ¹⁶¹	Inhalt/Erläuterungen	Prüfungen/Beispiele
:MT:	MT-Typ	an	3	F	P	Konstante „700“, „710“ oder „720“	
:M1:	SWIFT-Adresse der avisierenden Bank	an	11	V	K	BIC	8 oder 11 Stellen
:M2:	Klartextadresse der avisierenden Bank	an	4 x 35	V	P	Vorgegebene Reihenfolge ist Name, Straße/Postfach, Ort (Land)	
:M3:	Referenznummer der avisierenden Bank	an	16	V	P		
:M4:	Ansprechpartner bei der avisierenden Bank	an	35	V	P	Für eventuelle Rückfragen	
:M5:	Bestätigungsvermerk der avisierenden Bank	n	1	F	P	„1“ = bestätigt „2“ = unbestätigt	
:M6:	Information zum Bestätigungsvermerk	an	50 x 65	V	K	Ergänzung zum Feld :M5:	
:M7:	Hinweise der avisierenden Bank	an	100 x 65	V	K		
:M8:	Entgelt der avisierenden Bank	an	50 x 65	V	K		
:M9:	SWIFT-Adr. der eröffnenden Bank	an	11	V	K	BIC	8 oder 11 Stellen
:M10:	Klartextadresse der eröffnenden Bank	an	4 x 35	V	C	Vorgegebene Reihenfolge ist: Name, Straße/Postfach, Ort (Land). <i>Pflichtfeld bei Eröffnung (MT 700), Pflichtfeld bei Weiterleitung (MT 710), Pflichtfeld bei Übertragung (MT 720), falls Feld :M9: belegt</i>	

¹⁶⁰ an = alphanummerisch, n = numerisch, Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁶¹ P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten-format ¹⁶⁰	Länge in Bytes	variabel/fest	Kann/Pflicht ¹⁶¹	Inhalt/Erläuterungen	Prüfungen/Beispiele
:M11:	Akkreditivnummer der eröffnenden Bank	an	16	V	P		
:M12:	Eröffnungsdatum	n	8	F	P	Format JJJJMMTT	
:M13:	SWIFT-Adresse der zwischengeschalteten Bank	an	11	V	K	BIC	8 oder 11 Stellen
:M14:	Klartextadresse der zwischengeschalteten Bank	an	4 x 35	V	C	Vorgegebene Reihenfolge ist Name, Straße/Postfach, Ort (Land). <i>Pflichtfeld bei Weiterleitung (MT 710)</i>	
:M15:	Referenznummer der zwischen-geschalteten Bank	an	16	V	C	<i>Pflichtfeld bei Weiterleitung (MT 710)</i>	
:M16:	SWIFT-Adresse der übertragenden Bank	an	11	V	K	BIC	8 oder 11 Stellen
:M17:	Klartextadresse der übertragenden Bank	an	4 x 35	V	C	Vorgegebene Reihenfolge ist Name, Straße/Postfach, Ort (Land) <i>Pflichtfeld bei Übertragung (MT 720)</i>	
:M18:	Referenznummer der übertragen-den Bank	an	16	V	C	<i>Pflichtfeld bei Übertragung (MT 720)</i>	
:M19:	Avisierungsdatum	n	8	F	P	Format JJJJMMTT	
:M20:	Referenz des Kunden	an	16	V	K		
:M24:	Hinweis auf Informationskopie	an	20	F	C	Konstante „Unverbindliche Kopie“ <i>Pflichtfeld, falls Feld :A1: mit „EAI“ belegt (Informationskopie)</i>	
	Nachricht im SWIFT-Format MT 700, MT 710 oder MT 720 (ohne Header und Trailer)	an		V	P	MT 700/701, 710/711 oder 720/721 werden jeweils zusammengeführt (ohne Feld 27)	
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

DFÜ – Abkommen

Anlage 3 (Datenformate)

Akkreditivänderung 707

Feld-Nr.	Bezeichnung	Daten-format ¹⁶²	Länge in Bytes	variabel/fest	Kann/Pflicht ¹⁶³	Inhalt/Erläuterungen	Prüfungen/Beispiele
:MT:	MT-Typ	an	3	F	P	Konstante „707“	
:M1:	SWIFT-Adresse der avisierenden Bank	an	11	V	K	BIC	8 oder 11 Stellen
:M2:	Klartextadresse der avisierenden Bank	an	4 x 35	V	P	Vorgegebene Reihenfolge ist Name, Straße/Postfach, Ort (Land)	
:M3:	Referenznummer der avisierenden Bank	an	16	V	P		
:M4:	Ansprechpartner bei der avisierenden Bank	an	35	V	P	Für eventuelle Rückfragen	
:M5:	Bestätigungsvermerk der avisierenden Bank	n	1	F	K	„1“ = bestätigt „2“ = unbestätigt	
:M6:	Information zum Bestätigungsvermerk	an	50 x 65	V	K	Ergänzung zum Feld :M5:	
:M7:	Hinweise der avisierenden Bank	an	100 x 65	V	K		
:M8:	Entgelt der avisierenden Bank	an	50 x 65	V	K		
:M9:	SWIFT-Adresse der eröffnenden Bank	an	11	V	K	BIC	8 oder 11 Stellen
:M10:	Klartextadresse der eröffnenden Bank	an	4 x 35	V	C	Vorgegebene Reihenfolge ist Name, Straße/Postfach, Ort (Land) <i>Pflichtfeld, falls Feld :M9: belegt</i>	

¹⁶² an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁶³ P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten-format ¹⁶²	Länge in Bytes	variabel/fest	Kann/Pflicht ¹⁶³	Inhalt/Erläuterungen	Prüfungen/Beispiele
:M11:	Akkreditivnummer der eröffnenden Bank	an	16	V	P		
:M12:	Eröffnungsdatum	n	8	F	K	Format JJJJMMTT	
:M19:	Avisierungsdatum	n	8	F	P	Format JJJJMMTT	
:M20:	Referenz des Kunden	an	16	V	K		
:M21:	Änderungsdatum der eröffnenden Bank	n	8	F	P	Format JJJJMMTT	
:M22:	Änderungsnummer der avisierenden Bank	n	2	V	K		
:M24:	Hinweis auf Informationskopie	an	20	F	C	Konstante „Unverbindliche Kopie“ <i>Pflichtfeld, falls Feld :A1: mit „EAI“ belegt (Informationskopie)</i>	
	Nachricht im SWIFT-Format MT 707 (ohne Header und Trailer)	an		V	P		
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

DFÜ – Abkommen

Anlage 3 (Datenformate)

Freiformat 799

Feld-Nr.	Bezeichnung	Daten-format ¹⁶⁴	Länge in Bytes	variabel/fest	Kann/Pflicht ¹⁶⁵	Inhalt/Erläuterungen	Prüfungen/Beispiele
:MT:	MT-Typ	an	3	F	P	Konstante „799“	
:M3:	Referenznummer der avisierenden Bank	an	16	V	P		
:M11:	Akkreditivnummer der eröffnenden Bank	an	16	V	P		
:M20:	Referenz des Kunden	an	16	V	K		
:M23:	Kommentar der avisierenden Bank	an	30 x 65	V	K		
:M24:	Hinweis auf Informationskopie	an	20	F	C	Konstante „Unverbindliche Kopie“ <i>Pflichtfeld, falls Feld :A1: mit „EAI“ belegt (Informationskopie)</i>	
:79:	Freier Text	an	35 x 50	V	P		
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

¹⁶⁴ an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁶⁵ P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

Datenträgnachsatz Z

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁶⁶	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁶⁷	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:Z1:	Kennzeichnung Nachsatz	an	1	F	P	Konstante „Z“	
:Z2:	Anzahl der 700, 710 und 720	n	3	F	P		
:Z3:	Anzahl der 707	n	3	F	P		
:Z4:	Anzahl der 799	n	3	F	P		
:Z5:	Summe der Beträge über alle Währungen aus den Feldern :32B: der 700, 710, 720 und :34B: der 707	n	15	V	P	Rechenprozess ohne Nachkommastellen und Endsummenausgabe ohne Nach- kommastellen. Ist Feld :34B: aus 707 leer, wird der Wert „707“ addiert. Für jeden 799 wird der Wert „799“ addiert	
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

¹⁶⁶ an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁶⁷ P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

3.4.2 DTALC Import-Akkreditiveröffnungs- und Änderungsaufträge (Kunde an Bank)

Alle Felder inklusive Satzendeckennung werden mit <CR><LF> (X'0D0A') abgeschlossen.

Zugelassener Zeichencode ¹⁶⁸	Zeichen	Hexcode
Nummerische Zeichen	0 bis 9	X '30' - X '39'
Großbuchstaben	A bis Z	X '41' - X '5A'
<u>Sonderzeichen:</u>		
Leerzeichen	" "	X '20'
Punkt	" . "	X '2E'
Komma	" , "	X '2C'
Trennstrich	" - "	X '2D'
Schrägstrich	" / "	X '2F'
Pluszeichen	" + "	X '2B'
Doppelpunkt	" . "	X '3A'
Klammer auf	" ("	X '28'
Klammer zu	") "	X '29'
Hochkomma	" ' "	X '27'

Die Umlaute Ä, Ö; Ü sind wie AE, OE, UE und ß wie SS aufzuzeichnen.

Anzahl des Auftretens in logischer Datei	Element (jeweils mit Satzendeckennung)
1	Datenträgervorsatz AKK
0-n	Akkreditiveröffnungsauftrag 700 oder Akkreditivänderungsauftrag 707
0-n	Freiformat 799
1	Datenträgnachsatz Z

¹⁶⁸ Codierung gemäß DIN 66003 (Ausgabe Juni 1974), Code Tabelle 2, Deutsche Referenz Version.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Datenträgervorsatz AKK

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁶⁹	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁷⁰	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:A1:	Kennzeichnung Vorsatz	an	3	F	P	Konstante „AKK“	
:A2:	Bankleitzahl oder SWIFT-BIC	an	11	V	P	Bankleitzahl oder SWIFT-BIC des absen- denden Kreditinstitutes	:A2:25070000 oder :A2DEUTDE2H
:A3:	Kundennummer	an	23	V	P	Ordnungsnummer gemäß Vereinbarung mit dem sendenden Kreditinstitut (gegebenenfalls Kontonummer)	
:A4:	Auftraggeberdaten	an	4 x 35	V	P	Daten zum Feld :A3: Zeile 1 und 2: Name Zeile 3: Straße/Postfach Zeile 4: Ort	
:A5:	Auftragsdatum	n	8	F	P	Format:JJJJMMTT	Erstellungsdatum der Datei
:A6:	Bundesbankmeldung durch be- auftragtes Kreditinstitut	an	1	F	P	Konstante „N“	
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

¹⁶⁹ an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁷⁰ P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Akkreditiveröffnungsauftrag 700

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁷¹	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁷²	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:MT:	MT-Typ	an	3	F	P	Konstante „700“	
:M1:	Referenznummer des Kunden	an	16	V	P		
:M2:	Versandart	n	2	F	P	„01“ = Mittels Telekommunikation „02“ = Luftpostalisch ohne Voravis „03“ = Luftpostalisch mit Voravis per Telekommunikation „04“ = Mittels Kurierdienst ohne Voravis „05“ = Mittels Kurierdienst mit Voravis per Telekommunikation	
:M3:	Kurierdienst	an	35	V	C	Zu beauftragender Kurierdienst (soweit mög- lich)	Nur wenn Feld :M2: = „04“ oder „05“
:M4:	Ansprechpartner beim Kunden	an	35	V	K	Ansprechpartner für eventuelle Rückfragen	Telefonnummer
:M5:	ISO-Code der Kontonummer für die Inanspruchnahme	an	3	F	P	ISO-Code der Kontonummer für Belastung der Inanspruchnahme und Gebühren, sofern für Gebührenbelastung Feld :M8: nicht be- legt.	:M5:EUR
:M6:	Bankleitzahl/Kontonummer oder SWIFT-BIC/Kontonummer für Belastung der Inanspruchnahme	an	35	V	P	Bankleitzahl oder SWIFT-BIC und Konto- nummer für Belastung der Inanspruchnahme und Gebühren, sofern für Gebühren- belastung Feld :M8: nicht belegt.	:M6:25050000/7890 oder :M6:NOLADE2H/7890

¹⁷¹ an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁷² P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁷¹	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁷²	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:M7:	ISO-Code der Kontonummer für Gebühren	an	3	F	C	ISO-Code der Kontonummer für Belastung der Gebühren	:M7:EUR
:M8:	Bankleitzahl/Kontonummer oder SWIFT-BIC/Kontonummer für Belastung der Gebühren	an	35	V	C	Bankleitzahl oder SWIFT-BIC und Kontonummer für Belastung der Gebühren	:M8:25050000/7890 oder :M8:NOLADE2H/7890
:M9:	frühester Ausführungstermin	n	8	F	K	Format: JJJJMMTT	maximal 14 Tage nach Auftragsertei- lung „A5“
:M10:	Kostenverrechnungsschlüssel	n	2	F	P	„00“ = Gebührenteilung „01“ = alle Gebühren zu Lasten Auftraggeber „02“ = alle Gebühren zu Lasten Begünstigter „03“ = andere Regelung	
:M11:	Sonderregelung Kostenverrechnung	an	6 x 35	V	C		Pflichtfeld, falls Feld :M10: = „03“
:M12:	Sonstige Kunde-Bank-Informationen	an	6 x 35	V	K		
:20:	Referenznummer der eröffnenden Bank	an	16	V	K		
:40A:	Art des Akkreditives	an	24	V	P	erlaubte Codeworte: „IRREVOCABLE“ oder „IRREVOCABLE STANDBY“ oder „IRREVOCABLE TRANSFERABLE“ oder „REVOCABLE“ oder „REVOCABLE STANDBY“ oder „REVOCABLE TRANSFERABLE“ oder „IR- REVOC TRANS STANDBY“	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁷¹	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁷²	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:31D:	Datum und Ort des Verfalls				P		:31D:931029HANNOVE R
	Subfeld 1: Verfallsdatum	n	6	F		Format: JJMMTT	Darf nicht vor dem Datum in Feld :A5: im Datenträgervorsatz und vor dem Datum in Feld :44C: liegen
	Subfeld 2: Verfallsort	an	29	V			
:50:	Auftraggeberdaten	an	4 x 35	V	P	Name und Adresse des Auftraggebers	
:59:	Akkreditivbegünstigter					Kontonummer sowie Name und Anschrift des Akkreditivbegünstigten	:59:/ACC-1234865- 21789
	Subfeld 1: Kontonummer	an	35	V	K	:59:/34x	Prüfung: Konto- nummer darf nur vor- handen sein, wenn auch Feld :57a: vor- handen ist
	Subfeld 2: Akkreditivbegünstigter	an	4 x 35	V	P		
:32B:	Akkreditivwährung Akkreditivbetrag	an n	3 15	F V	P	ISO-Code Betrag maximal drei Nachkommastellen, Vor- und Nachkommastellen durch Komma getrennt	:32B:USD8795,75
:39A:	prozentuale Betragstoleranz	n	5	F	C	Format: nn/nn 1. Wert: positive Abweichung in Prozent 2. Wert: negative Abweichung in Prozent	:39A:05/08 Wenn dieses Feld belegt ist, darf Feld :39B: nicht belegt sein
:39B:	Maximalbetrag	an	13	V	C	erlaubtes Codewort: „NOT EXCEEDING“	Wenn dieses Feld belegt ist, darf Feld :39A: nicht belegt sein.
:39C:	zusätzlich gedeckte Beträge	an	4 x 35	V	K	zum Beispiel Frachtkosten, Zinsen, Versi- cherung	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁷¹	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁷²	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:41a:	benutzbar bei ... durch				P	a = Variante „A“ oder „D“ Adresse der Bank, bei der das Akkreditiv benutzbar sein soll. Subfeld 1, Variante „A“: SWIFT-BIC	wenn Subfeld 2 = „BY NEGOTIATION“, erhält Subfeld 1 je nach Konstellation des Akkreditives den Default-Wert: „ANY BANK“ oder „ANY BANK IN...“ (Stadt/ Land) oder die Ad- resse einer Bank, sofern das Akkreditiv bei einer bestimmten Bank benutzbar sein soll (Bank des Be- günstigten, Sonstige Bank).
:41A:	Subfeld 1: benutzbar bei	an	11	V			
:41D:	Subfeld 1: benutzbar bei	an	4 x 35	V		Subfeld 1, Variante „D“: Name, Straße, Ort	
:41A/D:	Subfeld 2: durch	an	14	V		Subfeld 2: erlaubte Codeworte „BY PAYMENT“ oder „BY ACCEPTANCE“ oder „BY NEGOTIATION“ oder „BY DEF PAYMENT“ oder „BY MIXED PYMT“	
:42C:	Tratten per	an	3 x 35	V	C	Spezifiziert die Wechselziehung zum Beispiel Drafts at ...	Belegung nur erlaubt, wenn Subfeld 2 von Feld :41D: ist <i>nicht</i> „BY DEF PAYMENT“ oder „BY MIXED PYMT“. Pflichtfeld, wenn Sub- feld 2 von Feld :41D: = „BY ACCEPTAN- CE“.
:42a:	Bezogener				C	a = Variante „A“ oder „D“ Name und Anschrift der bezogenen Bank	Belegung nur erlaubt, wenn Subfeld 2 von :41D: ist <i>nicht</i> „BY DEF PAYMENT“ oder „BY MIXED PYMT“.
:42A:	Bezogener	an	11	V		Variante „A“: SWIFT-BIC	Pflichtfeld, wenn Feld :42C: belegt ist
:42D:	Bezogener	an	4 x 35	V		Variante „D“: Name, Straße, Ort	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁷¹	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁷²	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:42M:	Mixed Payment Details	an	4 x 35	V	C	Nähere Spezifikation zu: „BY MIXED PYMT“ in Feld :41D:, Subfeld 2	Pflichtfeld, falls Feld :41D: = „BY MIXED PYMT“
:42P:	Deferred Payment Details	an	4 x 35	V	C	Nähere Spezifikation zu: „BY DEF PAYMENT“ in Feld :41D:, Subfeld 2	Pflichtfeld, falls Feld :41D: = „BY DEF PAYMENT“
:43P:	Teilverladung	an	35	V	K	erlaubte Codeworte: „ALLOWED“ oder „NOT ALLOWED“	
:43T:	Umladung	an	35	V	K	erlaubte Codeworte: „ALLOWED“ oder „NOT ALLOWED“	
:44A:	Versandort	an	65	V	K		
:44B:	Bestimmungsort	an	65	V	K		
:44C:	spätester Verladetag	n	6	F	K	Format: JJMMTT	darf nicht nach Ver- fallsdatum in Feld :31D: liegen
:44D:	Verladezeitraum	an	6 x 65	V	C	Belegung nur erlaubt, wenn Feld :44C: nicht belegt ist.	
:45A:	Warenbeschreibung	an	100 x 65	V	P	letzte Zeile der Warenbeschreibung ist die Lieferbedingung, z.B. „CIF-HAMBURG“	
:46A:	Dokumente	an	100 x 65	V	P	Die Dokumentenbeschreibung <i>sollte</i> wie folgt aufgebaut sein: 1. Rechnungsdokumente 2. Transportdokumente 3. Versicherungsdokumente 4. Sonstige Dokumente	
:47A:	Zusätzliche Bedingungen	an	50 x 65	V	K		
:48:	Dokumentenvorlagefrist	an	4 x 35	V	K		

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁷¹	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁷²	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:49:	Akkreditivbestätigung	an	7	F	P	erlaubte Codeworte: „WITHOUT“ oder „CONFIRM“ oder „MAY ADD“	
:57a:	Bank des Akkreditivbegünstigten					a = Variante „A“ oder „D“ Name und Anschrift der Bank des Akkreditivbegünstigten	
:57A:	Bank des Akkreditivbegünstigten	an	11	V	K	Variante „A“: SWIFT-BIC	
:57D:	Bank des Akkreditivbegünstigten	an	4 x 35	V	K	Variante „D“: Name, Straße, Ort	
:MLD:	Anzahl der nachfolgenden Melde- teile MT-TYP = „T“	n	3	F	P	Konstante „000“	
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

DFÜ – Abkommen

Anlage 3 (Datenformate)

Akkreditivänderungsauftrag 707

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁷³	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁷⁴	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:MT:	MT-Typ	an	3	F	P	Konstante „707“	
:M1:	Referenznummer des Kunden	an	16	V	P		
:M2:	Versandart	n	2	F	P	„01“ = Mittels Telekommunikation „02“ = Luftpostalisch ohne Voravis „03“ = Luftpostalisch mit Voravis per Telekommunikation „04“ = Mittels Kurierdienst ohne Voravis „05“ = Mittels Kurierdienst mit Voravis per Telekommunikation	
:M3:	Kurierdienst	an	35	V	C	zu beauftragender Kurierdienst (soweit möglich)	nur wenn Feld :M2: = „04“ oder „05“
:M4:	Ansprechpartner beim Kunden	an	35	V	K	Ansprechpartner für eventuelle Rückfragen	Telefonnummer
:M10:	Kostenverrechnungsschlüssel für Akkreditivänderung	n	2	F	P	„00“ = Gebührenteilung „01“ = alle Gebühren zu Lasten Auftraggeber „02“ = alle Gebühren zu Lasten Begünstigter „03“ = andere Regelung	
:M11:	Sonderregelung Kostenverrech- nung	an	6 x 35	V	C		Pflichtfeld, falls Feld :M10: = „03“
:M12:	Sonstige Kunde-Bank-Informationen	an	6 x 35	V	K		

¹⁷³ an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁷⁴ P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁷³	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁷⁴	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:20:	Referenznummer der eröffnenden Bank	an	16	V	P		
:26E:	Nummer der Änderung	N	2	F	K		
:59:	Akkreditivbegünstigter					Kontonummer sowie Name und Anschrift des Akkreditivbegünstigten vor der Änderung	:59:/ACC-1234865-21789 Prüfung: Kontonummer darf nur vorhanden sein, wenn auch Feld :57a: in der Eröffnung vorhanden ist.
	Subfeld 1: Kontonummer	an	35	V	K	:59:/34x	
	Subfeld 2: Akkreditivbegünstigter	an	4 x 35	V	P		
:31E:	Neuer Verfalltag	n	6	F	K	Format: JJMMTT	¹⁷⁵
:32B:	Akkreditivwährung Erhöhungsbetrag	an n	3 15	F V	C	ISO-Code Betrag maximal drei Nachkommastellen, Vor- und Nachkommastellen durch Komma getrennt	Feld :32B: oder :33B: muss belegt sein, falls :34B: belegt ist :32B:USD3000,50
:33B:	Akkreditivwährung Ermäßigungsbetrag	an n	3 15	F V	C	ISO-Code Betrag maximal drei Nachkommastellen, Vor- und Nachkommastellen durch Komma getrennt	Feld :32B: oder :33B: muss belegt sein, falls :34B: belegt ist :33B:USD3000,50
:34B:	Akkreditivwährung Akkreditivbetrag nach Änderung	an n	3 15	F V	C	ISO-Code Betrag maximal drei Nachkommastellen, Vor- und Nachkommastellen durch Komma getrennt	Pflichtfeld, falls Feld :32B: oder :33B: be- legt ist. :34B:USD13000,50 (bei Erhöhung) :34B:USD6999,50 (bei Ermäßigung) ¹⁷⁵

¹⁷⁵ Diese Felder dürfen bei einer Akkreditivänderung auf keinen Fall Daten des aktuellen Akkreditives enthalten. In einem MT 707 sind lediglich Änderungen gegenüber dem herausgelegten Akkreditiv anzuzeigen. Im Feld :34B: ist keine Änderung der Währung zulässig.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁷³	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁷⁴	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:39A:	prozentuale Betragstoleranz	n	5	F	C	Format: nn/nn 1. Wert: positive Abweichung in Prozent 2. Wert: negative Abweichung in Prozent	:39A:05/08 Wenn dieses Feld belegt ist, darf Feld :39B: nicht belegt sein ¹⁷⁵
:39B:	Maximalbetrag	an	13	V	C	erlaubtes Codewort: „NOT EXCEEDING“	Wenn dieses Feld belegt ist, darf Feld :39A: nicht belegt sein ¹⁷⁵
:39C:	zusätzlich gedeckte Beträge	an	4x35	V	K	zum Beispiel Frachtkosten, Zinsen, Versi- cherung	¹⁷⁵
:44A:	Versandort	an	65	V	K		¹⁷⁵
:44B:	Bestimmungsort	an	65	V	K		¹⁷⁵
:44C:	spätester Verladetag	n	6	F	K	Format: JJMMTT	darf nicht nach Ver- fallsdatum in Feld :31D: liegen ¹⁷⁵
:44D:	Verladezeitraum	an	6 x 65	V	C		Belegung nur erlaubt, wenn Feld :44C: nicht belegt ist ¹⁷⁵
:79:	Zusätzliche Bedingungen	an	35 x 50	V	K		¹⁷⁵
:MLD:	Anzahl der nachfolgenden Melde- teile MT-TYP = „T“	n	3	F	P	Konstante „000“	
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

DFÜ – Abkommen

Anlage 3 (Datenformate)

Freiformat 799

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁷⁶	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁷⁷	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:MT:	MT-Typ	an	3	F	P	Konstante „799“	
:M1:	Referenznummer des Kunden	an	16	V	P		
:20:	Referenznummer der eröffnenden Bank	an	16	V	P		
:79:	Freier Text	an	35 x 50	V	P		
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

¹⁷⁶ an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁷⁷ P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Datenträgnachsatz Z

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁷⁸	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁷⁹	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:Z1:	Kennzeichnung Nachsatz	an	1	F	P	Konstante „Z“	
:Z2:	Anzahl der Akkreditiveröffnungs- aufträge MT-Typ „700“	n	3	F	P		
:Z3:	Anzahl der Akkreditivänderungs- aufträge MT-Typ „707“	n	3	F	P		
:Z4:	Anzahl der freien Nachrichten MT-Typ „799“	n	3	F	P		
:Z5:	Anzahl der freien Meldeteile MT-Typ „T“	n	3	F	P	Konstante „000“	
:Z6:	Summe der Beträge über alle Währungen aus den Feldern :32B: der MT 700 und :34B: der MT 707	n	15	V	P	Rechenprozess ohne Nachkommastellen und End- summenausgabe ohne Nachkommastellen. Ist Feld :34B: aus 707 leer, wird der Wert „707“ ad- diert. Für jeden 799 wird der Wert „799“ addiert	
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

¹⁷⁸ an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁷⁹ P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

3.4.3 DTALCR Ausführungsbestätigungen von Import-Akkreditiveröffnungen und –änderungen (Bank an Kunde)

Alle Felder inklusive Satzendeckennung werden mit <CR><LF> (X'0D0A') abgeschlossen.

Zugelassener Zeichencode ¹⁸⁰	Zeichen	Hexcode
Nummerische Zeichen	0 bis 9	X '30' - X '39'
Großbuchstaben	A bis Z	X '41' - X '5A'
<u>Sonderzeichen:</u>		
Leerzeichen	" "	X '20'
Punkt	" ."	X '2E'
Komma	" ,"	X '2C'
Trennstrich	" -"	X '2D'
Schrägstrich	" /"	X '2F'
Pluszeichen	" +"	X '2B'
Doppelpunkt	" ."	X '3A'
Klammer auf	" ("	X '28'
Klammer zu	")"	X '29'
Hochkomma	" ' "	X '27'

Die Umlaute Ä, Ö; Ü sind wie AE, OE, UE und ß wie SS aufzuzeichnen.

Anzahl des Auftretens in logischer Datei	Element (jeweils mit Satzendeckennung)
1	Datenträgervorsatz AKB
0-n	Ausführungsbestätigung und Akkreditiveröffnung 700 oder Akkreditivänderung 707
0-n	Freiformat 799
1	Datenträgnachsatz Z

¹⁸⁰ Codierung gemäß DIN 66003 (Ausgabe Juni 1974), Code Tabelle 2, Deutsche Referenz Version.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Datenträgervorsatz AKB

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁸¹	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁸²	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:A1:	Kennzeichnung Vorsatz	an	3	F	P	Konstante „AKB“	
:A2:	Bankleitzahl oder SWIFT-BIC-Code	an	11	V	P	Bankleitzahl oder SWIFT-BIC des absendenden Kreditinstitutes	:A2:25070070 oder :A2:DEUTDE2H
:A3:	Kundennummer	an	23	V	P	Ordnungsnummer gemäß Vereinbarung mit dem absendenden Kreditinstitut (ggf. Konto- nummer)	
:A4:	Empfängerdaten	an	4 x 35	V	P	Zeile 1 und Zeile 2: Name Zeile 3: Straße/Postfach Zeile 4: Ort	
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

¹⁸¹ an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁸² P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Akkreditivavisierung 700

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁸³	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁸⁴	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:MT:	MT-Typ	an	3	F	P	Konstante „700“	
:M1:	Referenznummer des Kunden	an	16	V	P		:
:M2:	Versandart	an	2	F	P	„01“ = Mittels Telekommunikation „02“ = Luftpostalisch ohne Voravis „03“ = Luftpostalisch mit Voravis per Telekommunikation „04“ = Mittels Kurierdienst ohne Voravis „05“ = Mittels Kurierdienst mit Voravis per Telekommunikation	
:M3:	Kurierdienst	an	35	V	C	zu beauftragender Kurierdienst (soweit möglich)	Nur wenn Feld :m2: = „04“ oder „05“
:M4:	Ansprechpartner beim Kreditinsti- tut	an	35	V	K	Ansprechpartner für eventuelle Rückfragen	Telefonnummer
:M9:	Ausführungstermin	n	8	F	P	Format: JJJJMMTT	
:M12:	Sonstige Bank-Kunde-Informationen	an	6 x 35	V	K		
:M14:	Avisierende Bank	an	4 x 35	V	P	Name und Anschrift der Bank, die mit der Avisierung beauftragt wurde	
:20:	Referenznummer der eröffnenden Bank	an	16	V	P		

¹⁸³ an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁸⁴ P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁸³	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁸⁴	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:40A:	Art des Akkreditives	an	24	V	P	erlaubte Codeworte: „IRREVOCABLE“ oder „IRREVOCABLE STANDBY“ oder „IRREVOCABLE TRANSFERABLE“ oder „REVOCABLE“ oder „REVOCABLE STANDBY“ oder „REVOCABLE TRANSFERABLE“ oder „IR- REVOC TRANS STANDBY“	
:31C:	Datum der Akkreditiveröffnung	n	6	F	P	Format: JJMMTT	
:31D:	Datum und Ort des Verfalls				P		
	Subfeld 1: Verfallsdatum	n	6	F		Format: JJMMTT	
	Subfeld 2: Verfallsort	an	29	V			
:50:	Auftraggeberdaten	an	4 x 35	V	P	Name und Adresse des Auftraggebers	
:59:	Akkreditivbegünstigter					Kontonummer sowie Name und Anschrift des Akkreditivbegünstigten	:59:/ACC-1234865- 21789 Prüfung: Kontonum- mer darf nur vor- handen sein, wenn auch Feld :57a: vor- handen ist
	Subfeld 1: Kontonummer	an	35	V	K	:59:/34x	
	Subfeld 2: Akkreditivbegünstigter	an	4 x 35	V	P		
:32B:	Akkreditivwährung Akkreditivbetrag	an n	3 15	F V	P	ISO-Code Betrag maximal drei Nachkommastellen, Vor- und Nachkommastellen durch Komma getrennt	:32B:USD8795,75
:39A:	prozentuale Betragstoleranz	n	5	F	C	Format: nn/nn 1. Wert: positive Abweichung in Prozent 2. Wert: negative Abweichung in Prozent	:39A:05/08 Wenn dieses Feld belegt ist, darf Feld :39B: nicht belegt sein

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁸³	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁸⁴	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:39B:	Maximalbetrag	an	13	V	C	erlaubtes Codewort: „NOT EXCEEDING“	Wenn dieses Feld belegt ist, darf Feld :39A: nicht belegt sein.
:39C:	zusätzlich gedeckte Beträge	an	4 x 35	V	K	z.B. Frachtkosten, Zinsen, Versicherung	
:41a:	benutzbar bei ... durch				P	a = Variante „A“ oder „D“ Adresse der Bank, bei der das Akkreditiv benutzbar sein soll. Subfeld 1, Variante „A“: SWIFT-BIC	wenn Subfeld 2 = „BY NEGOTIATION“, erhält Subfeld 1 je nach Konstellation des Akkreditives den Default-Wert: „ANY BANK“ oder „ANY BANK IN...“ (Stadt/ Land) oder die Ad- resse einer Bank, sofern das Akkreditiv bei einer bestimmten Bank benutzbar sein soll (Bank des Be- günstigten, Sonstige Bank).
:41A:	Subfeld 1: benutzbar bei	an	11	V			
:41D:	Subfeld 1: benutzbar bei	an	4 x 35	V		Subfeld 1, Variante „D“: Name, Straße, Ort	
:41A/D:	Subfeld 2: durch	an	14	V		Subfeld 2: erlaubte Codeworte: „BY PAYMENT“ oder „BY ACCEPTANCE“ oder „BY NEGOTIATION“ oder „BY DEF PAYMENT“ oder „BY MIXED PYMT“	
:42C:	Tratten per	an	3 x 35	V	C	Spezifiziert die Wechselziehung zum Beispiel Drafts at ...	Belegung nur erlaubt, wenn Subfeld 2 von Feld :41D: ist <i>nicht</i> „BY DEF PAYMENT“ oder „BY MIXED PYMT“. Pflichtfeld, wenn Sub- feld 2 von Feld :41D: = „BY ACCEPTAN- CE“.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁸³	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁸⁴	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:42a:	Bezogener				C	a = Variante „A“ oder „D“ Name und Anschrift der bezogenen Bank	Belegung nur erlaubt, wenn Subfeld 2 von :41D: ist <i>nicht</i> „BY DEF PAYMENT“ oder „BY MIXED PYMT“.
:42A:	Bezogener	an	11	V		Variante „A“: SWIFT-BIC	Pflichtfeld, wenn Feld :42C: belegt ist
:42D:	Bezogener	an	4 x 35	V		Variante „D“: Name, Straße, Ort	
:42M:	Mixed Payment Details	an	4 x 35	V	C	Nähere Spezifikation zu: „BY MIXED PYMT“ in Feld :41D:, Subfeld 2	Pflichtfeld, falls Feld :41D: = „BY MIXED PYMT“
:42P:	Deferred Payment Details	an	4 x 35	V	C	Nähere Spezifikation zu: „BY DEF PAYMENT“ in Feld :41D:, Subfeld 2	Pflichtfeld, falls Feld :41D: = „BY DEF PAYMENT“
:43P:	Teilverladung	an	35	V	K	erlaubte Codeworte: „ALLOWED“ oder „NOT ALLOWED“	
:43T:	Umladung	an	35	V	K	erlaubte Codeworte: „ALLOWED“ oder „NOT ALLOWED“	
:44A:	Versandort	an	65	V	K		
:44B:	Bestimmungsort	an	65	V	K		
:44C:	spätester Verladetag	n	6	F	K	Format: JJMMTT	darf nicht nach Ver- fallsdatum in Feld :31D: liegen
:44D:	Verladezeitraum	an	6 x 65	V	C	Belegung nur erlaubt, wenn Feld :44C: nicht belegt ist.	
:45A:	Warenbeschreibung	an	100 x 65	V	P	letzte Zeile der Warenbeschreibung ist die Lieferbedingung, zum Beispiel „CIF-HAMBURG“	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁸³	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁸⁴	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:46A:	Dokumente	an	100 x 65	V	P	Die Dokumentenbeschreibung <i>solite</i> wie folgt aufgebaut sein: 1. Rechnungsdokumente 2. Transportdokumente 3. Versicherungsdokumente 4. Sonstige Dokumente	
:47A:	Zusätzliche Bedingungen	an	50 x 65	V	K		
:71B:	Gebührenregelung	an	6 x 35	V	P		
:48:	Dokumentenvorlagefrist	an	4 x 35	V	K		
:53a:	Remboursbank					a = Variante „A“ oder „D“ Name und Anschrift der Remboursbank	
:53A:	Remboursbank	an	11	V	K	Variante „A“: SWIFT-BIC	
:53D:	Remboursbank	an	4 x 35	V	K	Variante „D“: Name, Straße, Ort	
:78:	Weisungen an die zahlende, akzeptierende oder negoziierende Bank	an	12 x 65	V	K		
:57a:	Bank des Akkreditivbegünstigten					a = Variante „A“ oder „D“ Name und Anschrift der Bank des Akkreditivbegünstigten	
:57A:	Bank des Akkreditivbegünstigten	an	11	V	K	Variante „A“: SWIFT-BIC	
:57D:	Bank des Akkreditivbegünstigten	an	4 x 35	V	K	Variante „D“: Name, Straße, Ort	
:72:	Mehrzweckfeld	an	6 x 35	V	K		
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

DFÜ – Abkommen

Anlage 3 (Datenformate)

Akkreditivänderung 707

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁸⁵	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁸⁶	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:MT:	MT-Typ	an	3	F	P	Konstante „707“	
:M1:	Referenznummer des Kunden	an	16	V	P		
:M2:	Versandart	n	2	F	P	„01“ = Mittels Telekommunikation „02“ = Luftpostalisch ohne Voravis „03“ = Luftpostalisch mit Voravis per Telekommunikation „04“ = Mittels Kurierdienst ohne Voravis „05“ = Mittels Kurierdienst mit Voravis per Telekommunikation	
:M3:	Kurierdienst	an	35	V	C	zu beauftragender Kurierdienst (soweit möglich)	nur wenn Feld :M2: = „04“ oder „05“
:M4:	Ansprechpartner beim Kreditinsti- tut	an	35	V	K	Ansprechpartner für eventuelle Rückfragen	
:M9:	Ausführungstermin	n	8	F	P	Format: JJJJMMTT	
:M12:	Sonstige Bank-Kunde-Informationen	an	6 x 35	V	K		
:20:	Referenznummer der eröffnenden Bank	an	16	V	P		
:30:	Datum der Änderung	an	6	F	P	Format: JJMMTT	
:26E:	Nummer der Änderung	n	2	F	K		

¹⁸⁵ an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁸⁶ P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁸⁵	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁸⁶	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:59:	Akkreditivbegünstigter					Kontonummer sowie Name und Anschrift des Akkreditivbegünstigten	:59:/ACC-1234865-21789
	Subfeld 1: Kontonummer	an	35	V	K	:59:/34x	
	Subfeld 2: Akkreditivbegünstigter	an	4 x 35	V	P		
:31E:	Neuer Verfalltag	n	6	F	K	Format: JJMMTT	
:32B:	Akkreditivwährung	an	3	F	C	ISO-Code	Feld :32B: oder :33B: muss belegt sein, falls
	Erhöhungsbetrag	n	15	V		Betrag maximal drei Nachkommastellen, Vor- und Nachkommastellen durch Komma getrennt	:34B: belegt ist :32B:USD3000,50
:33B:	Akkreditivwährung	an	3	F	C	ISO-Code	Feld :32B: oder :33B: muss belegt sein, falls
	Ermäßigungsbetrag	n	15	V		Betrag maximal drei Nachkommastellen, Vor- und Nachkommastellen durch Komma getrennt	:34B: belegt ist :33B:USD3000,50
:34B:	Akkreditivwährung	an	3	F	C	ISO-Code	Pflichtfeld, falls Feld :32B: oder :33B: belegt ist.
	Akkreditivbetrag nach Änderung	n	15	V		Betrag maximal drei Nachkommastellen, Vor- und Nachkommastellen durch Komma getrennt	:34B:USD13000,50 (bei Erhöhung) :34B:USD6999,50 (bei Ermäßigung)
:39A:	prozentuale Betragstoleranz	n	5	F	C	Format: nn/nn 1. Wert: positive Abweichung in Prozent 2. Wert: negative Abweichung in Prozent	:39A:05/08 Wenn dieses Feld belegt ist, darf Feld :39B: nicht belegt sein
:39B:	Maximalbetrag	an	13	V	C	erlaubtes Codewort: „NOT EXCEEDING“	Wenn dieses Feld belegt ist, darf Feld :39A: nicht belegt sein
:39C:	zusätzlich gedeckte Beträge	an	4x35	V	K	z.B. Frachtkosten, Zinsen, Versicherung	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁸⁵	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁸⁶	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:44A:	Versandort	an	65	V	K		
:44B:	Bestimmungsort	an	65	V	K		
:44C:	spätester Verladetag	n	6	F	K	Format: JJMMTT	darf nicht nach Ver- fallsdatum in Feld :31D: liegen
:44D:	Verladezeitraum	an	6 x 65	V	C		Belegung nur erlaubt, wenn Feld :44C: nicht belegt ist
:79:	Zusätzliche Bedingungen	an	35 x 50	V	K		
:72:	Information Bank an Bank	an	6 x 35	V	K		
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

DFÜ – Abkommen

Anlage 3 (Datenformate)

Freiformat 799

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁸⁷	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁸⁸	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:MT:	MT-Typ	an	3	F	P	Konstante „799“	
:M1:	Referenznummer des Kunden	an	16	V	P		
:20:	Referenznummer der eröffnenden Bank	an	16	V	P		
:79:	Freier Text	an	35 x 50	V	P		
–	Satzendekennung	an	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

¹⁸⁷ an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁸⁸ P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Datenträgnachsatz Z

Feld-Nr.	Bezeichnung	Daten- for- mat ¹⁸⁹	Länge in Bytes	variabel/ fest	Kann/ Pflicht ¹⁹⁰	Inhalt/ Erläuterungen	Prüfungen/ Beispiele
:Z1:	Kennzeichnung Nachsatz	A	1	F	P	Konstante „Z“	
:Z2:	Anzahl der Akkreditiveröffnungen MT-Typ „700“	N	3	F	P		
:Z3:	Anzahl der Akkreditivänderungen MT-Typ „707“	N	3	F	P		
:Z4:	Anzahl der freien Nachrichten MT-Typ „799“	N	3	F	P		
:Z6:	Summe der Beträge über alle Währungen aus den Feldern :32B: der MT 700 und :34B: der MT 707	N	15	V	P	Rechenprozess ohne Nachkommastellen und Endsummenausgabe ohne Nachkom- mastellen. Ist Feld :34B: aus 707 leer, wird der Wert „707“ addiert. Für jeden 799 wird der Wert „799“ addiert	
–	Satzendekennung	A	1	F	P	Trennstrich (X'2D')	Code nach ISO 8859

¹⁸⁹ an = alphanummerisch, n = numerisch. Alphanummerische Werte im ASCII-Format werden linksbündig eingestellt und rechts mit Blanks (X'20') aufgefüllt. Numerische Felder werden rechtsbündig angeordnet und links mit Nullwerten (X'30') aufgefüllt.

¹⁹⁰ P = Pflichtfeld, K = Kannfeld, C = Conditionalfeld (Bedingung in Spalte „Inhalt/Erläuterungen“)

3.5 Tageskontoauszugsinformationen

Für alle SWIFT-Formate gilt, soweit nichts anderes definiert, der SWIFT-Zeichensatz:

Der S.W.I.F.T.-Zeichensatz ist ein Subset von ISO 8859:

	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	ç	£	¤	¥	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

Die geschweiften Klammern gehören zwar zum Zeichensatz und sind als Feldbegrenzungen zulässig, dürfen aber nicht im Text einer Nachricht von Benutzer zu Benutzer verwendet werden.

3.5.1 MT 940 Kontoauszugsdaten

„Transaction Report“; basiert auf SWIFT „Standards Release Guide“, Stand: Oktober 1998

- **Übersicht** (ohne konstante Felder)

Folge	Sub- folge	Tag	Sta- tus ¹⁹¹	Inhalt
		:20:	M	Auftragsreferenznummer
		:21:	K	Bezugsreferenznummer
		:25:	M	Kontobezeichnung
		:28C:	M	Auszugsnummer
		:60a:	M	Anfangssaldo
			K	Wiederholungszyklus
		:61:	K	Umsatz
		:86:	K	Mehrzweckfeld
		:62a:	M	Schlussaldo
		:64:	K	Aktueller Valutensaldo
		:65:	K	Zukünftige Valutensalden
		:86:	K	Mehrzweckfeld

- **Belegungsrichtlinien**

Folge	Sub- folge	Tag	Name	For- mat ¹⁹²	Län- ge	Sta- tus ¹⁹¹	An- zahl	Inhalt/Bemerkungen
		:20:	Auftragsreferenznummer			M	1	
			Tag			M	1	„:20:“
			Referenz	x	..16	M	1	Referenznummer, die vom Sender als eindeutige Kennung für die Nachricht vergeben wurde (z.B. als Referenz auf stornierte Nachrichten). Die Referenz darf nicht mit "/" starten oder enden; darf nicht "/" enthalten
		:21:	Bezugsreferenznummer			K	1	
			Tag			M	1	„:21:“

¹⁹¹ M = Pflichtfeld, K = Kannfeld

¹⁹² a = alpha (erlaubt sind „A“-„Z“), c = character (erlaubt sind „A“-„Z“ und „0“-„9“), d = dezimal (Fließkommazahl, der Vorkommaanteil muss wenigstens ein Zeichen enthalten, ein Dezimalkomma ist Pflicht und in der maximalen Länge enthalten), n = numerisch (erlaubt sind die Ziffern 0-9), x = alphanumerisch (erlaubt sind alle Zeichen aus dem SWIFT-Zeichensatz)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 192	Län- ge	Sta- tus ¹ 91	An- zahl	Inhalt/Bemerkungen
			Referenz	x	..16	M	1	Die Referenz darf nicht mit "/" starten oder enden; darf nicht "/" enthalten
		:25:	Kontobezeichnung			M	1	
			Tag			M	1	„:25:“
			Bank	x	..35	M	1	xxxxxxxxxx/Konto-Nr. oder xxxxxxxx/Konto-Nr. oder xxxxxxxxxxxx/IBAN wobei xxxxxxxxxxxx = SWIFT-Code xxxxxxxx = Bankleitzahl Konto-Nr. = max. 23 Stellen (ggf. mit Währung)
		:28C:	Auszugsnummer			M	1	
			Tag			M	1	„:28C:“
			Auszugsnummer	n	..5	M	1	falls eine Auszugsnummer nicht unterstützt wird, ist „0“ einzustellen
			Konstante			K	1	„/“, falls Blattnummer belegt
			Blattnummer	n	..3	K	1	beginnend mit „1“
		:60a:	Anfangssaldo			M	1	
			Option F					bei Anfangssaldo
			Tag			M	1	„:60F:“
			Soll/Haben-Kennung	a	1	M	1	„C“ = Credit (Habensaldo) „D“ = Debit (Sollsaldo)
			Buchungsdatum	n	6	M	1	JJMMTT = Buchungsdatum des Saldos oder '0' beim ersten Auszug
			Währung	a	3	M	1	Währungsschlüssel gem. ISO 4217
			Betrag	d	..15	M	1	
			Option M					bei Zwischensaldo
			Tag			M	1	„:60M:“
			Soll/Haben-Kennung	a	1	M	1	„C“ = Credit (Habensaldo) „D“ = Debit (Sollsaldo)
			Buchungsdatum	n	6	M	1	JJMMTT = Buchungsdatum des Saldos oder '0' beim ersten Auszug
			Währung	a	3	M	1	Währungsschlüssel gem. ISO 4217
			Betrag	d	..15	M	1	

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 192	Län- ge	Sta- tus ¹ 91	An- zahl	Inhalt/Bemerkungen
↓ Beginn des Wiederholungszyklus gemäß SWIFT								
		:61:	Umsatz			K	1	
			Tag			M	1	„:61:“
			Datum	n	6	M	1	Valuta (JJMMTT)
			Buchungsdatum	n	4	K	1	MMTT
			Soll/Haben-Kennung	a	..2	M	1	„C“ = Haben „D“ = Soll „RC“ = Storno Haben „RD“ = Storno Soll
			Währungsart	a	1	K	1	dritte Stelle der Wäh- rungsbezeichnung, falls sie zur Unterscheidung notwendig ist
			Betrag	d	..15	M	1	in Kontowährung
			Konstante	a	1	M	1	„N“
			Buchungsschlüssel	c	3	M	1	Codes: „BOE“ = Bill of exchange (Sichttratte) „BRF“ = Brokerage fee (Wertpapierprovision) „CHG“ = Gebühren und andere Auslagen „CHK“ = Schecks „CLR“ = Geldbriefe/ Scheckeinreichungen „COL“ = Inkassi (bei An- gabe eines Hauptbeträ- ges) „COM“ = Provision „DCR“ = Dokumentenak- kreditiv (bei Angabe eines Hauptbetrages) „DIV“ = Dividenden-Be- zugsrechte „EQA“ = Equivalent a- mount (Gegenwertver- rechnung) „ECK“ = Eurocheques „FEX“ = Foreign exchange (Devisenhandel) „INT“ = Interest (Zinsen) „LBX“ = Schließfach „LDP“ = Loan deposit (Darlehen) „MSC“ = Miscellaneous (Verschiedenes) „RTI“ = Returned item (Rückbuchung) „SEC“ = Wertpapiere (bei Angabe eines Hauptbeträ- ges)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat ¹⁹²	Län- ge	Sta- tus ⁹¹	An- zahl	Inhalt/Bemerkungen
								„STO“ = Standing order (Dauerauftrag) „TCK“ = Reiseschecks „TRF“ = Transfer (Übertrag) „VDA“ = Berichtigung des Wertstellungsdatums (wenn eine Buchung unter einem falschen Datum ausgeführt wurde, wird dieser Code für die Korrektur verwendet - es folgt die korrekte Buchung mit dem entsprechenden Code)
			Referenz	x	..16	M	1	Kundenreferenz. Bei Nichtbelegung wird „NONREF.“ eingestellt, zum Beispiel bei Schecknummer oder DTA-Satz A, Feld 10
			Konstante			K	1	„/“, falls Bankreferenz vorhanden
			Bankreferenz	x	..16	K	1	Bankreferenz (z.B. bei DTA: Feld 6b)
			Konstante			K	1	<CR><LF>, falls „Weitere Informationen“ vorhanden
			Konstante			K	1	„/“, falls „Weitere Informationen“ vorhanden
			Weitere Informationen/ Ursprungsbetrag und Gebührenbetrag ¹⁹³	x	..34	K	1	Währungsart und Umsatzbetrag in Ursprungswährung (original currency amount) in folgendem Format: /OCMT/3a..15d/ sowie Währungsart und Gebührenbetrag (charges) in folgendem Format: /CHGS/3a..15d/ 3a = 3-stelliger Währungscode gemäß ISO 4217 ..15d = Betrag mit Komma als Dezimalzeichen (gemäß SWIFT-Konvention)

¹⁹³ Die Belegung des Feldes wird 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.

	:86:	Mehrzweckfeld			K	1	
		Tag			M	1	„:86:“
		Freier Text	x	..65	M	6	siehe Belegungsrichtlinien des MT 940 einschließlich der zugehörigen Geschäftsvorfallcodes Die Zeilen werden mit <CR><LF> getrennt.
	↑ Ende des Wiederholungszyklus gemäß SWIFT						
	:62a:	Schlussaldo			M	1	
		Option F					bei Schlussaldo
		Tag			M	1	„:60F:“
		Soll/Haben-Kennung	a	1	M	1	“C” = Credit (Habensaldo) “D” = Debit (Sollsaldo)
		Buchungsdatum	n	6	M	1	JJMMTT
		Währung	a	3	M	1	Währungsschlüssel gem. ISO 4217
		Betrag	d	..15	M	1	
		Option M					bei Zwischensaldo
		Tag			M	1	„:60M:“
		Soll/Haben-Kennung	a	1	M	1	“C” = Credit (Habensaldo) “D” = Debit (Sollsaldo)
		Buchungsdatum	n	6	M	1	JJMMTT = Buchungsdatum des Saldos oder '0' beim ersten Auszug
		Währung	a	3	M	1	Währungsschlüssel gem. ISO 4217
		Betrag	d	..15	M	1	
	:64:	Aktueller Valutensaldo			K	1	
		Tag			M	1	„:64:“
		Soll/Haben-Kennung	a	1	M	1	“C” = Credit (Habensaldo) “D” = Debit (Sollsaldo)
		Buchungsdatum	n	6	M	1	JJMMTT
		Währung	a	3	M	1	Währungsschlüssel gem. ISO 4217
		Betrag	d	..15	M	1	
	:65:	Zukünftige Valutensalden			K	6	
		Tag			M	1	„:65:“
		Soll/Haben-Kennung	a	1	M	1	“C” = Credit (Habensaldo) “D” = Debit (Sollsaldo)
		Buchungsdatum	n	6	M	1	JJMMTT
		Währung	a	3	M	1	Währungsschlüssel gem. ISO 4217
		Betrag	d	..15	M	1	
	:86:	Mehrzweckfeld			K	1	
		Tag			M	1	„:86:“

DFÜ – Abkommen

Anlage 3 (Datenformate)

		Freier Text	x	..65	K	6	Es dürfen nur unstrukturierte Informationen eingestellt werden. Es dürfen keine Informationen, die auf einzelne Umsätze bezogen sind, eingestellt werden. Die Zeilen werden mit <CR><LF> getrennt.
--	--	-------------	---	------	---	---	---

- **Strukturierte Belegung des Feldes 86¹⁹⁴**

Feld-schlüssel	Name	Format	Länge	Status	Anzahl	Bemerkungen
	Geschäftsvorfall-Code	numerisch	3	M	1	gemäß Anlage
00	Buchungstext	alpha	..27	K	1	
10	Primanoten-Nr.	alphanum	..10	K	1	
20-29	Verwendungszweck ¹⁹⁵	alphanum	..27	K	10	
30	BLZ Überweisender / Zahlungsempfänger	numerisch	..12	K	1	
31	Konto-Nr. Überweisender / Zahlungsempfänger	numerisch	..24	K	1	
32-33	Name Überweisender / Zahlungsempfänger	alphanum	..27	K	2	
34	Textschlüsselergänzung	numerisch	3	K	1	
60-63	Verwendungszweck	alphanum	..27	K	4	

Das Steuerzeichen "?" steht vor jedem Feldschlüssel.

¹⁹⁴ 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 definierten Geschäftsvorfall-Codes eingestellt werden.

¹⁹⁵ Soweit das Kreditinstitut 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 SWIFT-Konvention)

Soweit 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/

- **Beispiel**

Folge	Sub-folge	Beispiel
		:20:1234567 :21:9876543210 :25:10020030/1234567 :28C:5/1 :60F:C021101EUR2187,95
		:61:0211011102DR800,NSTONONREF//55555 :86:008?00DAUERAUFTRAG?100599?20Miete November?3010020030?31234567 ?32MUELLER?34339
		:61:0211021102CR3000,NTRFNONREF//55555 :86:051?00UEBERWEISUNG?100599?20Gehalt Oktober ?21Firma Mustermann GmbH?3050060400?31084756 4700?32MUELLER?34339
		:62F:C021131EUR4387,95 -

- **Geschäftsvorfallcodes**

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 betriebs-spezifische 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 = Kreditgeschäft

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.

Code	Geschäftsvorfall
------	------------------

0XX	INLANDSZAHLUNGSVERKEHR
-----	------------------------

001	Inhaberscheck (nicht eurocheque)
-----	----------------------------------

002	Orderscheck
-----	-------------

003	DM-Reisescheck
-----	----------------

004	Lastschrift (Abbuchungsverfahren)
-----	-----------------------------------

005	Lastschrift (Einzugsermächtigungsverfahren)
-----	---

006	sonstige Einzugspapiere
-----	-------------------------

008	Dauerauftrag Belastung
-----	------------------------

009	Retourenhülle (Lastschrift) für Einzugspapier, Rücklastschrift aus Datenträgeraustausch, Lastschrift (Rückbelastung) - DTA -
-----	--

010	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
--	--

Code	Geschäftsvorfall
	Ersatzstück für verlorengegangenen Scheck
011	eurocheque
012	Zahlungsanweisung zur Verrechnung
013	EU-Standardüberweisung
014	Lastschrift für Fremdwährungs-eurocheque / Lastschrift für über die GZS abgewickelte Auslandsschecks
015	Auslandsüberweisung ohne Meldeteil
017	Überweisung beim neutralen Überweisungs-/Zahlscheinvordruck mit prüfziffergesicherten Zuordnungsdaten
018	Überweisung beim neutralen Überweisungs-/Zahlscheinvordruck
019	Überweisung beim neutralen Spenden-Überweisungs-/Zahlscheinvordruck
020	Überweisung
051	Überweisungsgutschrift
052	Dauerauftragsgutschrift
053	Lohn-, Gehalts-, Rentengutschrift
054	Vermögenswirksame Leistungen
056	Überweisung öffentlicher Kassen
058	Bank-an-Bank-Zahlung (Überweisungsgutschrift)
059	Retourenhülle (Gutschrift) für unanbringliche Überweisung, Gutschrift (Rücküberweisung) - DTA -
063	Überweisungsgutschrift - EU-Standardüberweisung
065	Überweisungsgutschrift (Auslandsüberweisung ohne Meldeteil)
066	Gutschrift aus Scheckeinreichung E.v. (Exportscheckabwicklung über GZS)
067	Gutschrift beim neutralen Überweisungs-/Zahlscheinvordruck mit prüfziffergesicherten internen Zuordnungsdaten
068	Gutschrift beim neutralen Überweisungs-/Zahlscheinvordruck EZÜ
069	Gutschrift beim neutralen Spenden-Überweisungs-/Zahlscheinvordruck EZÜ
070	Scheckeinreichung
071	Lastschrifteinreichung
072	Wechseleinreichung
073	Wechsel
074	TC (Scheckbelastung)
075	Scheck BSE
076	Telefonauftrag
077	BTX-Überweisung
078	Überweisung (Versorgungsbezüge)
079	Sammler
080	Gehalt
081	Vergütung
082	Einzahlungen
083	Auszahlungen
084	BTX-Einzugsauftrag
087	Überweisung mit Festvaluta
088	Überweisungsgutschrift mit Festvaluta
089	drahtliche Überweisung mit Festvaluta
090	drahtliche Überweisungsgutschrift mit Festvaluta
091	DATA-Einreichung Überweisungen
092	DATA-Einreichung Lastschriften
093	Diskont-Wechsel

Code	Geschäftsvorfall
094	Rediskont-Wechsel
095	Aval (Inland)
096	Kontoübertrag (Soll)
097	Kontoübertrag (Haben)
098	GeldKarte (Umsatz Elektronische Geldbörse)
099	GeldKarte (Händlerprovision für Zahlungsgarantie)
1XX	INLANDSZAHLUNGSVERKEHR
	Reserve
2XX	AUSLANDSGESCHÄFT
201	Zahlungsauftrag
202	Auslandsvergütung
203	Inkasso
204	Akkreditiv
205	Aval
206	Auslandsüberweisung
207	zunächst frei
208	Rembourse
209	Zahlung per Scheck
210	Zahlung über elektronische Medien
211	Zahlungseingang über elektronische Medien
212	Dauerauftrag
213	Lastschrift-Einzug aus dem Ausland
214	Dokumenten-Inkasso (Import)
215	Dokumenten-Inkasso (Export)
216	Wechsel-Inkasso (Import)
217	Wechsel-Inkasso (Export)
218	Import-Akkreditiv
219	Export-Akkreditiv
220	Gutschrift e.V. eines Auslands-Schecks
221	Gutschrift Auslands-Scheck-Inkasso
222	Belastung Auslands-Scheck
223	Belastung Auslands-ec-Scheck
224	Sorten-Ankauf
225	Sorten-Verkauf
3XX	WERTPAPIERGE SCHÄFT
301	Inkasso
302	Kupon/Dividenden
303	Effekten
304	Übertrag
305	Namensschuldverschreibung
306	Schuldschein
307	Wertpapierzeichnung
308	Handel von Bezugsrechten
309	Handel von Bonusrechten
310	Handel von Optionen

Code	Geschäftsvorfall
311	Termingeschäfte
320	Gebühren für Wertpapiergeschäfte
321	Depotgebühren
330	Erträge aus Wertpapieren
340	Gutschrift für fällige Wertpapiere
399	Storno
4XX	D E V I S E N G E S C H Ä F T
401	Kassedevisen
402	Termindevisen
403	Reisedevisen
404	Devisenscheck
405	Finanzinnovationen
406	
407	
408	
409	
410	
411	Devisenkassa-Kauf
412	Devisenkassa-Verkauf
413	Devisentermin-Kauf
414	Devisentermin-Verkauf
415	FW-Tagegeld-Aktiv
416	FW-Tagegeld-Passiv
417	FW-Termingeld-Aktiv
418	FW-Termingeld-Passiv
419	Call-Geld-Aktiv
420	Call-Geld-Passiv
421	Optionen
422	Swap
423	Edelmetall-Ankauf
424	Edelmetall-Verkauf
5XX	M A O B E
6XX	K R E D I T G E S C H Ä F T
601	Einzug von Raten/Annuitäten
602	Überweisung von Raten/Annuitäten
603	Tilgung
604	Darlehenszinsen
605	Darlehenszinsen mit Nebenleistungen
7XX	R E S E R V E
8XX	S O N S T I G E
801	Scheckkarte
802	Scheckheft
803	Depotverwahrung
804	Dauerauftragsgebühren

Code	Geschäftsvorfall
805	Abschluss
806	Porto/Zustellgebühren
807	Preise/Spesen
808	Gebühren
809	Provisionen
810	Mahngebühren
811	Kreditkosten
812	Stundungszinsen
813	Disagio
814	Zinsen
815	kapitalisierte Zinsen
816	Zinssatzänderung
817	Zinsberichtigung
818	Abbuchung
819	Bezüge
820	Übertrag
821	Telefon
822	Auszahlplan
823	Festgeld
824	Leihgeld
825	Universaldarlehn
826	dynamisches Sparen
827	Überschusssparen
828	Sparbrief
829	Sparplan
830	Bonus
831	alte Rechnung
832	Hypothek
833	Cash Concentrating - Buchung Hauptkonten
834	Cash Concentrating - Avisinformation für Nebenkonten
835	sonstige nicht definierte GV-Arten
836	Reklamationsbuchung
888	Umbuchung wegen Euro-Umstellung
899	Storno
9XX	UNSTRUKTURIERTER INHALT
997	Depotaufstellung -> MT 571
999	Unstrukturierte Belegung des Mehrzweckfeldes Feld '86'

3.5.2 MT 942 Kontoumsatzavis

„Interim Transaction Report“; basiert auf SWIFT „Standards Release Guide“, Stand: Oktober 1998

- Übersicht** (ohne konstante Felder)

Folge	Sub- folge	Tag	Sta- tus 196	Inhalt
		:20:	M	Auftragsreferenznummer
		:21:	K	Bezugsreferenznummer
		:25:	M	Kontobezeichnung
		:28C:	M	Auszugsnummer
		:34F:	M	Mindestbetrag (Kleinster Betrag der gemeldeten Umsätze)
		:34F:	K	Mindestbetrag (Kleinster Betrag der gemeldeten Haben-Umsätze)
		:13:	M	Erstellungszeitpunkt
			K	Wiederholungszyklus
		:61:	K	Umsatz
		:86:	K	Mehrzweckfeld
		:90D:	K	Anzahl und Summe der Soll-Buchungen
		:90C:	K	Anzahl und Summe der Haben-Buchungen

- Belegungsrichtlinien**

Folge	Sub- folge	Tag	Name	For- mat 197	Län- ge	Sta- tus ¹ 96	An- zahl	Inhalt/Bemerkungen
		:20:	Auftragsreferenznummer			M	1	
			Tag			M	1	„:20:“
			Referenz	x	..16	M	1	Referenznummer, die vom Sender als eindeutige Kennung für die Nachricht vergeben wurde (z.B. als Referenz auf stornierte Nachrichten). Die Referenz darf nicht mit "/" starten oder enden; darf nicht "/" enthalten
		:21:	Bezugsreferenznummer			K	1	
			Tag			M	1	„:21:“
			Referenz	x	..16	M	1	Die Referenz darf nicht mit "/" starten oder enden;

¹⁹⁶ M = Pflichtfeld, K = Kannfeld

¹⁹⁷ a = alpha (erlaubt sind „A“-„Z“), c = character (erlaubt sind „A“-„Z“ und „0“-„9“), d = dezimal (Fließkommazahl, der Vorkommaanteil muss wenigstens ein Zeichen enthalten, ein Dezimalkomma ist Pflicht und in der maximalen Länge enthalten), n = numerisch (erlaubt sind die Ziffern 0-9), x = alphanumerisch (erlaubt sind alle Zeichen aus dem SWIFT-Zeichensatz)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 197	Län- ge	Sta- tus ¹ 96	An- zahl	Inhalt/Bemerkungen
								darf nicht "/" enthalten
		:25:	Kontobezeichnung			M	1	
			Tag			M	1	„:25:“
			Bank	x	..35	M	1	xxxxxxxxxx/Konto-Nr. oder xxxxxxxx/Konto-Nr. oder xxxxxxxxxxxx/IBAN wobei xxxxxxxxxx = SWIFT- Code xxxxxxx = Bankleitzahl Konto-Nr. = max. 23 Stel- len (ggf. mit Währung)
		:28C:	Auszugsnummer			M	1	
			Tag			M	1	„:28C:“
			Auszugsnummer	n	..5	M	1	falls eine Auszugsnummer nicht unterstützt wird, ist „0“ einzustellen
			Konstante			K	1	„/“, falls Blattnummer be- legt
			Blattnummer	n	..3	K	1	beginnend mit „1“
		:34F:	Mindestbetrag			M	1	Kleinster Betrag der ge- meldeten Umsätze. Falls sich kleinster Soll- und Haben-Umsatz unter- scheiden, sind beide Fel- der :34F: zu belegen
			Tag			M	1	„:34F:“
			Währung	a	3	M	1	gemäß ISO 4217
			Soll/Haben-Kennung	a	1	K	1	„D“, falls Soll-Umsatz, sonst leer
			Betrag	d	..15	M	1	
		:34F:	Mindestbetrag			K	1	Kleinster Betrag der ge- meldeten Haben-Umsätze
			Tag			M	1	„:34F:“
			Währung	a	3	M	1	gemäß ISO 4217
			Soll/Haben-Kennung	a	1	M	1	„C“
			Betrag	d	..15	M	1	
		:13:	Erstellungszeitpunkt			M	1	
			Tag			M	1	„:13:“
			Datum	n	6	M	1	JJMMTT
			Uhrzeit	n	4	M	1	hhmm

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 197	Län- ge	Sta- tus ¹ 96	An- zahl	Inhalt/Bemerkungen
↓ Beginn des Wiederholungszyklus gemäß SWIFT								
		:61:	Umsatz			K	1	
			Tag			M	1	„61.“
			Datum	n	6	M	1	JJMMTT
			Buchungsdatum	n	4	K	1	MMTT
			Soll/Haben-Kennung	a	..2	M	1	„C“ = Haben „D“ = Soll „RC“ = Storno Haben „RD“ = Storno Soll
			Währungsart	a	1	K	1	dritte Stelle der Wäh- rungsbezeichnung, falls sie zur Unterscheidung notwendig ist
			Betrag	d	..15	M	1	in Kontowährung
			Konstante	a	1	M	1	„N“
			Buchungsschlüssel	c	3	M	1	Codes: „BOE“ = Bill of exchange (Sichtratte) „BRF“ = Brokerage fee (Wertpapierprovision) „CHG“ = Gebühren und andere Auslagen „CHK“ = Schecks „CLR“ = Geldbriefe/ Scheckeinreichungen „COL“ = Inkassi (bei An- gabe eines Hauptbetrages) „COM“ = Provision „DCR“ = Dokumenten- akkreditiv (bei Angabe eines Hauptbetrages) „DIV“ = Dividenden-Be- zugsrechte „EQA“ = Equivalent a- mount (Gegenwertver- rechnung) „ECK“ = Eurocheques „FEX“ = Foreign exchange (Devisenhandel) „INT“ = Interest (Zinsen) „LBX“ = Schließfach „LDP“ = Loan deposit (Darlehen) „MSC“ = Miscellaneous (Verschiedenes) „RTI“ = Returned item (Rückbuchung) „SEC“ = Wertpapiere (bei Angabe eines Hauptbetrages)

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 197	Län- ge	Sta- tus ¹ 96	An- zahl	Inhalt/Bemerkungen
								„STO“ = Standing order (Dauerauftrag) „TCK“ = Reiseschecks „TRF“ = Transfer (Übertrag) „VDA“ = Berichtigung des Wertstellungsdatums (wenn eine Buchung unter einem falschen Datum ausgeführt wurde, wird dieser Code für die Korrektur verwendet - es folgt die korrekte Buchung mit dem entsprechenden Code)
			Referenz	x	..16	M	1	Kundenreferenz. Bei Nichtbelegung wird „NONREF“ eingestellt, zum Beispiel bei Schecknummer oder DTA-Satz A, Feld 10
			Konstante			K	1	„/“, falls Bankreferenz vorhanden
			Bankreferenz	x	..16	K	1	Bankenreferenz (z.B. bei DTA: Feld 6b)
			Konstante			K	1	<CR><LF>, falls „Weitere Informationen“ vorhanden
			Konstante			K	1	„/“, falls „Weitere Informationen“ vorhanden
			Weitere Informationen/ Ursprungsbetrag und Gebührenbetrag ¹⁹⁸	x	..34	K	1	Währungsart und Umsatzbetrag in Ursprungswährung (original currency amount) in folgendem Format: /OCMT/3a..15d/ sowie Währungsart und Gebührenbetrag (charges) in folgendem Format: /CHGS/3a..15d/ 3a = 3-stelliger Währungscode gemäß ISO 4217 ..15d = Betrag mit Komma als Dezimalzeichen (gemäß SWIFT-Konvention)
		:86:	Mehrzweckfeld			K	1	

¹⁹⁸ Die Belegung des Feldes wird 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.

DFÜ – Abkommen

Anlage 3 (Datenformate)

Folge	Sub- folge	Tag	Name	For- mat 197	Län- ge	Sta- tus ¹ 96	An- zahl	Inhalt/Bemerkungen
			Tag			M	1	„:86:“
			Informationen	x	.. 390	M	1	siehe Belegungsrichtlinien des MT 940 einschließlich der zugehörigen Ge- schäftsvorfallcodes
↑ Ende des Wiederholungszyklus gemäß SWIFT								
		:90D:	Anzahl und Summe der Soll-Buchungen			K	1	
			Tag			M	1	„:90D:“
			Anzahl Soll-Buchungen	n	..5	M	1	
			Währung	a	3	M	1	gemäß ISO 4217
			Soll-Betrag	d	..15	M	1	
		:90C:	Anzahl und Summe der Haben-Buchungen			K	1	
			Tag			M	1	„:90C:“
			Anzahl Haben- Buchungen	n	..5	M	1	
			Währung	a	3	M	1	gemäß ISO 4217
			Haben-Betrag	d	..15	M	1	

- **Beispiel**

Folge	Sub- folge	Beispiel
		:20:1234567 :21:9876543210 :25:10020030/1234567 :28C:4/1 :34F:EURD800, :34F:EURC3000, :13:0211031245
		:61:0211011102DR800,NSTONONREF//55555 :86:008?00DAUERAUFTRAG?100599?20Miete Novem ber?3010020030?31234567 ?32MUELLER?34339 :61:9911021102CR3000,NTRFNONREF//55555 :86:051?00UEBERWEISUNG?100599?20Gehalt Oktob er ?21Firma Mustermann GmbH?3050060400?31084756 4700?32MUELLER?34339
		:90D:1EUR800, :90C:1EUR3000, -