

---

**FinTS**

**Financial Transaction Services**

- Schnittstellenspezifikation -

---

***Anlagen***

Herausgeber:

Bundesverband deutscher Banken e.V., Berlin

Deutscher Sparkassen- und Giroverband e.V., Bonn/Berlin

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

Bundesverband Öffentlicher Banken Deutschlands e.V., Berlin

Version: 4.0

Stand: 09.07.2004

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

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

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

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

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

Dieses Dokument kann im Internet abgerufen werden unter <http://www.fints.org>.

## ***Versionsführung***

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

Name	Organisation	Datum	Version	Dokumente	Anmerkungen
	SIZ	19.11.2003	4.0 final draft 01	FinTS_4.0_Anlagen.doc	
	SIZ	02.04.2004	4.0 final draft 02	FinTS_4.0_Anlagen.doc	
	SIZ	09.07.2004	4.0	FinTS_4.0_Anlagen.doc	keine Änderungen

## ***Änderungen gegenüber der Vorversion:***

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

Ifd. Nr.	Kapitel	Kapitelnummer	Ken-nung <sup>1</sup>	Art <sup>2</sup>	Beschreibung
1					

---

<sup>1</sup> nur zur internen Zuordnung

<sup>2</sup> F = Fehler; Ä = Änderung; K = Klarstellung; E = Erweiterung

Financial Transaction Services (FinTS) Dokument: Anlagen	Version: 4.0	Kapitel: I
Kapitel: <b>TRANSPORTMEDIENSPEZIFISCHE FESTLEGUNGEN</b> Abschnitt: Inhaltsverzeichnis	Stand: 09.07.2004	Seite: 1

## ***Inhaltsverzeichnis***

<b>I. TRANSPORTMEDIENSPEZIFISCHE FESTLEGUNGEN.....</b>	<b>3</b>
<b>I.1 HTTP .....</b>	<b>4</b>
<b>I.2 SMTP .....</b>	<b>7</b>
<b>I.3 Sonstige Kommunikationsdienste .....</b>	<b>9</b>
<b>I.4 Codierung.....</b>	<b>10</b>
 <b>II. Zulässige Kombinationen von Kommunikationsart, Transportprotokoll und Sicherheitsverfahren .....</b>	 <b>11</b>
 <b>III. Börsenplatzcodierungen.....</b>	 <b>13</b>
 <b>IV. Berechnung der Prüfziffer für interne Zuordnungsdaten (Kunden-Referenznummer) .....</b>	 <b>15</b>
<b>IV.1 Rechengang .....</b>	<b>16</b>
<b>IV.2 Beispiel .....</b>	<b>17</b>
 <b>V. LÄNDERKENNZEICHEN UND WÄHRUNGSCODES .....</b>	 <b>18</b>
 <b>VI. Europäische Kontenadressierung .....</b>	 <b>19</b>
 <b>VII. Verweise auf verwendete Dokumente .....</b>	 <b>25</b>

Kapitel: I	Version: 4.0	Financial Transaction Services (FinTS) Dokument: Anlagen
Seite: 2	Stand: 09.07.2004	Kapitel: <b>TRANSPORTMEDIENSPEZIFISCHE FESTLEGUNGEN</b> Abschnitt: Inhaltsverzeichnis

## ***Abbildungsverzeichnis***

Abbildung 1: Kommunikationsart, Transportprotokoll und Sicherheitsverfahren..... 12

Financial Transaction Services (FinTS) Dokument: Anlagen		Version: 4.0	Kapitel: I
Kapitel: TRANSPORTMEDIENSPEZIFISCHE FESTLEGUNGEN Abschnitt: HTTP		Stand: 09.07.2004	Seite: 3

## I. TRANSPORTMEDIENSPEZIFISCHE FESTLEGUNGEN

---

Obwohl FinTS grundsätzlich unabhängig von darunter liegenden Kommunikationsschichten ist, müssen doch bestimmte Festlegungen für die zu liefernden Netze getroffen werden, um FinTS multibankfähig und einheitlich zu definieren.

Hierbei handelt es sich um folgende Aspekte:

- Einschränkung der Kombinationsmöglichkeit von Protokollen, die für die gesicherte Übertragung von FinTS-Nachrichten zugelassen werden.
- Festlegung von verwendeten Parametern.
- Abbilden von FinTS-Kommunikationsabläufen auf die darunter liegenden Strukturen.

Wenn eines der nachfolgend beschriebenen Protokolle eine ausdrücklich als zulässig gekennzeichnete Transportverschlüsselung bietet, ist diese alternativ oder zusätzlich zur Verwendung verschlüsselter FinTS-Nachrichten (HBCI-Sicherheit) einsetzbar. Sollte die Transportverschlüsselung zur Verschlüsselung von bereits verschlüsselten FinTS-Nachrichten eingesetzt werden, ist die Transportverschlüsselung nicht relevant.

Eine in einem übermittelten Datagramm angegebene asynchrone Rückantwortadresse (vgl. [Formals], Abschnitt *II.7 Asynchrone Kommunikationsverfahren (Datagramme)* und [Syntax]), die von der durch das Transportverfahren vorgegebene Rückantwortadresse abweicht, wird bevorzugt benutzt.

Zur Zeit sind die folgenden Transportdienste beschrieben:

- HTTP (zulässige Transportverschlüsselung: SSL)
- SMTP

Kapitel:	I	Version:	4.0	Financial Transaction Services (FinTS) Dokument:	Anlagen
Seite:	4	Stand:	09.07.2004	Kapitel:	TRANSPORTMEDIENSPEZIFISCHE FESTLEGUNGEN
				Abschnitt:	HTTP

## I.1 HTTP

Realisierung Kreditinstitut: verpflichtend

Realisierung Kundensystem: verpflichtend

Der Transport von FinTS-Nachrichten über das „Hypertext Transfer Protocol“ (HTTP) stellt ein dialogorientiertes Verfahren zwischen Benutzer und Kreditinstitut dar. Die Kommunikation wird über die für HTTP bzw. HTTPS standardisierten Ports 80 bzw. 443 abgewickelt, so dass der Austausch von Nachrichten auch mit Kundenprodukten, die hinter einer Firewall lokalisiert sind, problemlos möglich ist.



Hersteller sollten ihre Produkte so flexibel gestalten, dass auch andere als die oben genannten Ports für die Kommunikation genutzt werden können.



Die Kommunikation erfolgt ausschließlich über HTTP/1.1 [RFC 2616]. FinTS-Nachrichten des Benutzers werden als Rumpf eines HTTP-Requests mittels der POST-Methode an das Kreditinstitut übertragen. Dieses sendet die Kreditinstitutsnachrichten im Rumpf einer HTTP-Response. Es werden immer vollständige FinTS-Nachrichten übertragen, eine Aufteilung in mehrere Requests bzw. Responses findet nicht statt. Wenn in Antworten des Kreditinstituts ein Statuscode geliefert wird, der nicht zwischen 200 und 299 (jeweils einschließlich) liegt, muss das Kundenprodukt dies als Fehler betrachten und die Kommunikation abbrechen.

Als MIME-Medientyp wird `application/vnd.fints` verwendet.

Die Kommunikation zwischen Benutzer und Kreditinstitut kann durch die SSL-Transportverschlüsselung gesichert werden. Dabei muss mindestens SSL Version 3.0 verwendet werden. SSL kann nach Vereinbarung zwischen den Kommunikationspartnern eine HBCI-Verschlüsselung vollständig ersetzen. Die Verwendung von SSL kann alternativ oder zusätzlich zur Verwendung verschlüsselter FinTS-Nachrichten erfolgen.



Um für den Benutzer sicherzustellen, dass er bei einer durch SSL gesicherten Kommunikation wirklich mit dem Kreditinstitut verbunden ist, sollte Server-Zertifizierung eingesetzt werden.

Bei der Kommunikation über HTTP zwischen Benutzer und Kreditinstitut besteht keine permanente Verbindung zwischen den Kommunikationspartnern, d. h. die Zugehörigkeit einzelner Nachrichten zu einer Kommunikation kann nur anhand der Kundenreferenz ermittelt werden. Die Kundenreferenz sollte nach den in [Formals], Abschnitt II.15.3 *Empfehlung für die Bildung von Kommunikationsreferenzen* angegebenen Regeln erfolgen.



Financial Transaction Services (FinTS) Dokument: Anlagen	Version: 4.0	Kapitel: I
Kapitel: TRANSPORTMEDIENSPEZIFISCHE FESTLEGUNGEN Abschnitt: HTTP	Stand: 09.07.2004	Seite: 5



Das Kundenprodukt muss die Kommunikation mit dem Kreditinstitut über einen auf Kundenseite angesiedelten Proxy unterstützen. Dabei ist mittels geeigneter Parameterbelegung sicherzustellen, dass die Daten nicht über zwischengeschaltete Caches gespeichert werden.

Kundenprodukte müssen weiterhin eine ggf. vom Proxy geforderte Proxy-Authentifikation unterstützen.

Im Folgenden wird exemplarisch die Kommunikation zwischen Benutzer und Kreditinstitut vorgestellt. Das Kundenprodukt sendet bei der Kommunikation über HTTP/1.1 einen Request nach folgendem Muster:

```
POST fints.kredinst.de/fints/in HTTP/1.1
Host: fints.kredinst.de
Pragma: no-cache
Cache-Control: no cache
Content-Length: nnn
Content-Type: application/vnd.fints; charset="UTF-8"

<ReqMsg>
...
</ReqMsg>
```

Dabei ist in `<ReqMsg/>` eine gültige FinTS-Nachricht nach der vorliegenden Spezifikation einzusetzen. Für den Platzhalter `nnn` ist die Länge der Nachricht einzustellen. Als Zeichensatzcodierung ist ausschließlich UTF-8 zulässig.

Im Unterschied zur Kommunikation über HTTP/1.0 ist bei HTTP/1.1 zusätzlich zum `no-cache-Pragma`, `Cache-Control: no-cache` und `,Host: fints.kredinst.de'` anzugeben:

Das Kreditinstitut beantwortet die Nachricht des Benutzers nach der Bearbeitung mit einer HTTP-Response nach folgendem Muster:

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Length: mmm
Content-Type: application/vnd.fints; charset="UTF-8"

<RespMsg>
...
</RespMsg>
```

Auch die Antwort ist ausschließlich in HTTP 1.1 angegeben. Zu beachten ist, dass auch der Server `,Cache-Control: no-cache'` einstellt und als Zeichensatzcodierung UTF-8 verwendet.

Kapitel: I	Version: 4.0	Financial Transaction Services (FinTS) Dokument: Anlagen
Seite: 6	Stand: 09.07.2004	Kapitel: TRANSPORTMEDIENSPEZIFISCHE FESTLEGUNGEN Abschnitt: HTTP



Eine Komprimierung der FinTS-Nachrichten über *Content-Encoding*, wie sie seit HTTP 1.1 möglich ist, wird nicht vorgenommen, weil FinTS von sich aus die Möglichkeit bietet, Nachrichten vor der Verschlüsselung zu komprimieren. Eine Komprimierung von bereits komprimierten oder verschlüsselten Daten wäre nicht sinnvoll. Bei SSL-gesicherter Übertragung wird die Komprimierung implizit vorgenommen.

Financial Transaction Services (FinTS) Dokument: Anlagen	Version: 4.0	Kapitel: I
Kapitel: TRANSPORTMEDIENSPEZIFISCHE FESTLEGUNGEN Abschnitt: SMTP	Stand: 09.07.2004	Seite: 7

## I.2 SMTP

Realisierung Kreditinstitut: freigestellt

Realisierung Kundensystem: freigestellt

Dieses Transportverfahren stellt ein datei- und nachrichtenorientiertes Verfahren dar, bei dem FinTS-Nachrichten per E-Mail [RFC 821] zwischen Benutzer und Kreditinstitut ausgetauscht werden. Somit ist es z. B. in Situationen, in denen keine permanente Kommunikationsverbindung zwischen Kundenprodukt und Kreditinstitut aufgebaut werden soll oder kann, trotzdem möglich, Bankgeschäfte mittels FinTS abzuwickeln.

Bei der Kommunikation werden FinTS-Datagramme als normales E-Mail-Attachment nach [RFC2045] und [RFC2046] versendet. In einer E-Mail können mehrere FinTS-Datagramme versendet werden, für jedes Datagramm ist ein eigenes Attachment zu verwenden. Für das Attachment wird der MIME-Medientyp `application/vnd.fints` verwendet. Ein Content-Transfer-Encoding für das Attachment ist zulässig, wobei die FinTS-Datagramme in UTF-8-Kodierung vorliegen müssen.

```
Content-Type: multipart/mixed; boundary=="_51C1256DC_"
...
--=_51C1256DC_=
Content-Type: application/vnd.fints; charset="UTF-8"Content-
transfer-encoding: base64
...
```

Das Betreff-Feld und der Rumpf der E-Mail (bis auf das FinTS-Attachment) werden vom Kreditinstitut ignoriert. Somit ist es nicht möglich, Verarbeitungshinweise oder sonstige Daten über diesen Weg an das Kreditinstitut zu übermitteln.



Das Kundenprodukt kann z. B. zu Archivierungszwecken im Betreff-Feld der E-Mail nur für das Produkt selbst relevante Informationen unterbringen. Aus Datenschutzgründen muss aber darauf geachtet werden, dass hier keine sensiblen Daten preisgegeben werden.



Das Kreditinstitut sollte – obwohl es den Betreff einer E-Mail nicht weiterverarbeitet – im Betreff-Feld der Antwort-E-Mail den Inhalt des Betreff-Feldes der Benutzernachricht widerspiegeln. Dabei kann der Feldinhalt aber um ein Präfix wie z. B. „Antwort:“ oder „Re:“ erweitert werden.

Kapitel: I	Version: 4.0	Financial Transaction Services (FinTS) Dokument: Anlagen
Seite: 8	Stand: 09.07.2004	Kapitel: TRANSPORTMEDIENSPEZIFISCHE FESTLEGUNGEN Abschnitt: SMTP

Eine Kreditinstitutsantwort, die nicht zugestellt werden konnte, wird vom Kreditinstitut nicht gepuffert oder erneut gesendet<sup>1</sup>, da dies einen sehr hohen Verwaltungsaufwand bedeuten würde. Der Benutzer hat über die üblichen Mechanismen wie das Abholen des Statusprotokolls oder die Synchronisierung bzgl. der Kundenreferenz die Möglichkeit, sich beim Kreditinstitut nach dem Status seiner Auftragsnachricht zu erkundigen.

Es ist zu beachten, dass eine innerhalb einer Benutzernachricht angegebene Rückantwortadresse die aus der E-Mail entnommene Antwortadresse übersteuern kann, so dass der Benutzer nicht zwingend eine Antwort-E-Mail des Kreditinstituts an die Absenderadresse der E-Mail bekommt.

---

<sup>1</sup> Davon unbenommen sind die Mechanismen, die bei SMTP ohnehin vorgesehen sind, um bei kurzzeitigen Serverausfällen E-Mails zumindest für einen bestimmten Zeitraum zu puffern, um später einen weiteren Versuch zu unternehmen, diese E-Mail zuzustellen.

Financial Transaction Services (FinTS) Dokument: Anlagen		Version: 4.0	Kapitel: I
Kapitel: TRANSPORTMEDIENSPEZIFISCHE FESTLEGUNGEN Abschnitt: Sonstige Kommunikationsdienste		Stand: 09.07.2004	Seite: 9

### **I.3 Sonstige Kommunikationsdienste**

Wird die Kommunikation über einen bisher nicht erfassten Kommunikationsdienst angestrebt, so sind zur Sicherstellung der Multibankfähigkeit vorab alle weiteren Spezifikationen durch den ZKA einheitlich festzulegen.

Kapitel: I	Version: 4.0	Financial Transaction Services (FinTS) Dokument: Anlagen
Seite: 10	Stand: 09.07.2004	Kapitel: TRANSPORTMEDIENSPEZIFISCHE FESTLEGUNGEN Abschnitt: Codierung

## I.4 Codierung

Die Codierung der Kommunikationswege erfolgt nach folgender Vorschrift:Code	Kommunikationsweg
3	HTTPS
4	SMTP
5	HTTP
6	SOAP mit HTTP-Binding

*Tabelle 1: Codierung der Kommunikationswege*

Financial Transaction Services (FinTS) Dokument: Anlagen	Version: 4.0	Kapitel: II
Kapitel: Zulässige Kombinationen von Kommunikationsart, Transportprotokoll und Sicherheitsverfahren	Stand: 09.07.2004	Seite: 11

## II. ZULÄSSIGE KOMBINATIONEN VON KOMMUNIKATIONSART, TRANSPORTPROTOKOLL UND SICHERHEITSVERFAHREN

Als zulässige Kommunikationsarten, über die ein Benutzer mit einem Kreditinstitut FinTS-Nachrichten austauschen kann, sind die synchrone Kommunikation (Dialog) und die asynchrone Kommunikation (Datagramme) in [Formals], Abschnitt *II.5 Unterstützte Kommunikationsverfahren im Überblick* beschrieben worden. Hiervon sollten beide Seiten bestimmte Transport- und Sicherheitsverfahren verpflichtend unterstützen, andere sind optional.

Der Begriff der „Verpflichtung“ ist unter dem Aspekt der Multibankfähigkeit als dringende Empfehlung zu verstehen, ohne deren Einhaltung eine ZKA-weit einheitliche Verwendung von FinTS nicht möglich ist. Dies bedeutet, dass ein Institut bzw. ein Kundensystem eine der folgenden Kombinationen unterstützen sollte, um einen multibankfähigen FinTS-Einsatz zu ermöglichen:

	Kundensystem	Kreditinstitut
<b>Kommunikationsart:</b>	synchron	synchron
<b>Transportprotokoll:</b>	HTTPS	HTTPS
<b>Sicherheitsverfahren:</b>	HBCI-RDH-3 und PIN/TAN	HBCI-RDH-3 und / oder PIN/TAN

*Tabelle 2: Empfehlungen für Transport- und Sicherheitsverfahren*



Für Kundenprodukte wird dringend empfohlen, aus Gründen der Multibankfähigkeit, die beiden Sicherheitsverfahren HBCI RDH-3 und PIN/TAN parallel zu unterstützen.

### Kommunikationsart

Die synchrone Kommunikation muss aus den o. g. Gründen von jedem Institut verpflichtend unterstützt werden. Die asynchrone Kommunikation ist optional.

### Transportprotokolle

Die zulässigen Transportprotokolle für den synchronen Fall sind HTTP und HTTPS wie in den vorangegangenen Kapiteln beschrieben. Hiervon ist HTTPS für beide Seiten verpflichtend. Die übrigen Protokolle sind optional.

Soll asynchrone Kommunikation unterstützt werden, so ist momentan SMTP das hierfür zulässige Transportprotokoll und damit verpflichtend bei Unterstützung von asynchroner Kommunikation.

In Kombination mit den unterschiedlichen Sicherheitsverfahren, die in FinTS zulässig sind, sind nicht alle Transportprotokolle sinnvoll einsetzbar. So sind Verfahren ohne Verschlüsselung (wie das PIN/TAN-Verfahren) nur über HTTPS sinnvoll einsetzbar, da nur hier eine Transportverschlüsselung verwendet werden kann, die die fehlende Verschlüsselung ersetzt. Über alle übrigen Transportkanäle wäre die Vertraulichkeit der Nachrichten nicht sichergestellt.

Auch würde die Kombination RDH-3 über HTTPS eine doppelte Verschlüsselung bedeuten. Empfohlen wird hier, entweder die Kombination „RDH-3 über HTTP“ oder die Kombination „RDH-3 über HTTPS ohne FinTS-Verschlüsselung“ zu unterstützen.

Kapitel: II	Version: 4.0	Financial Transaction Services (FinTS) Dokument: Anlagen
Seite: 12	Stand: 09.07.2004	Kapitel: Zulässige Kombinationen von Kommunikationsart, Transportprotokoll und Sicherheitsverfahren

### Sicherheitsverfahren

Von den zulässigen HBCI-Sicherheitsverfahren ist RDH-3 für beide Seiten verpflichtend. Die übrigen Verfahren sind optional.

Neben HBCI-RDH-3 kann zusätzlich oder ggf. auch alternativ das Sicherheitsverfahren PIN/TAN angeboten werden (vgl. Tabelle 2).

Die obigen Angaben sind in *Abbildung 1: Kommunikationsart, Transportprotokoll und Sicherheitsverfahren* noch einmal grafisch dargestellt. Die Verwendung von SOAP mit HTTP-Binding als zusätzlicher Layer auf Nachrichtenebene ist darüber hinaus möglich wie in [Syntax], Abschnitt VI. *WEBSERVICES* beschrieben.

Sicherheitsprofil \ Kommunikationsverfahren	synchron		asynchron
	HTTP	HTTPS	SMTP
DDV-1..2	X	X	X
RDH-1	X	X	X
RDH-2	X	X	X
RDH-3	X	X	X
RDH-4	X	X	X
PIN/TAN	-	X	-

X anwendbar  
 -- nicht anwendbar  
 X anwendbar, ggf. ohne FinTS-Verschlüsselung

*Abbildung 1: Kommunikationsart, Transportprotokoll und Sicherheitsverfahren*



Financial Transaction Services (FinTS) Dokument: Anlagen	Version: 4.0	Kapitel: III
Kapitel: Börsenplatzcodierungen Abschnitt:	Stand: 09.07.2004	Seite: 13

### III. BÖRSENPLATZCODIERUNGEN

Ausgewählte Börsenplätze und zugehöriger MIC-Code gemäß ISO 10383. Falls am angegebenen Börsenplatz mehrere Börsen mit unterschiedlichem MIC-Code existieren, ist in Klammern jeweils der Name der Börse angegeben, auf den sich der MIC-Code bezieht.

Deutsche Börsenplätze	Code
Berlin	XBER
Bremen	XBRE
Düsseldorf	XDUS
Frankfurt	XFRA
Hamburg	XHAM
Hannover	XHAN
München	XMUN
Stuttgart	XSTU
XETRA	XETR
EUREX	XEUR

Europäische Börsenplätze	Code
Amsterdam (Amsterdam Exchanges)	XAMS
Antwerpen	XANT
Athen	XATH
Barcelona	XBAR
Bern	XBRN
Bilbao	XBIL
Bordeaux	XBOR
Bratislava	XBRA
Budapest	XBUD
Brüssel (Société de la Bourse des Valeurs)	XBRU
Brüssel (EASDAQ)	XEAS
Dublin (Irish Stock Exchange)	XDUB
Helsinki (Helsinki Stock Exchange)	XHEL
Istanbul	XIST
Kopenhagen (Kobenhavns Fondsbørs)	XCSE
Lille	XLIL
Lissabon	XLIS

Europäische Börsenplätze	Code
Ljubljana	XLJU
London (London Stock Exchange)	XISE
London (London International Financial Futures and Options Exchange)	XLIF
Luxemburg	XLUX
Lyon	XLYO
Madrid (Bolsa de Madrid)	XMAD
Mailand	XMIL
Marseille	XMAR
Nancy	XNAY
Nantes	XNAN
Nicosia	XCYS
Oslo	XOSL
Paris (Société des Bourses Francaises)	XPAR
Prag	XPRA
Reykjavik	XICE
Rom (Mercato Italiano Futures)	XMIF
Sofia	XBUL
Stockholm	XSSE
Valencia	XVAL
Warschau	XWAR
Valletta	XMAL
Wien (Wiener Wertpapierbörse)	XVIE
Wien (Österreichische Termin- und Optionsbörse)	XOTB
Zagreb	XZAG
Zürich (Schweizer Börse)	XSWX
Zürich (ISMA)	XISM

Kapitel: III	Version: 4.0	Financial Transaction Services (FinTS) Dokument: Anlagen
Seite: 14	Stand: 09.07.2004	Kapitel: Börsenplatzcodierungen Abschnitt:

Internationale Börsenplätze (Auswahl)	Code
Bangkok	XBKK
Boston	XBOS
Buenos Aires	XBUE
Chicago (Chicago Stock Exchange)	XCHI
Hongkong (Stock Exchange of Hongkong)	XHKG
Johannesburg (Johannesburg Stock Exchange)	XJSE
Kuala Lumpur (Kuala Lumpur Stock Exchange)	XKLS
México	XMEX
Montreal (Montreal Exchange)	XMON
Moskau	XMOS
New York (American Stock Exchange)	XASE

Internationale Börsenplätze (Auswahl)	Code
New York (New York Stock Exchange)	XYNS
New York (New York Futures Exchange)	XYNYF
Rio de Janeiro	XRIO
San Francisco (Pacific Stock Exchange)	XPSE
São Paulo (Bolsa de Valores de São Paulo)	XBSP
Shanghai (Shanghai Stock Exchange)	XSHG
Singapur (Stock Exchange of Singapur)	XSES
Sydney (Australian Stock Exchange)	XASX
Tokio (Tokyo Stock Exchange)	XTKS
Toronto (Toronto Stock Exchange)	XTSE

Financial Transaction Services (FinTS) Dokument: Anlagen	Version: 4.0	Kapitel: IV
Kapitel: Berechnung der Prüfziffer für interne Zuordnungsdaten (Kunden-Referenznummer)	Stand: 09.07.2004	Seite: 15

## **IV. BERECHNUNG DER PRÜFZIFFER FÜR INTERNE ZUORDNUNGSDATEN (KUNDEN-REFERENZNUMMER)<sup>1</sup>**

---

(nach DIN ISO 7064, MOD 11,10)

---

<sup>1</sup> Entnommen aus „Richtlinien für einheitliche Zahlungsverkehrsvordrucke und Merkblätter für neutrale Zahlungsverkehrsvordrucke“.

Kapitel: IV	Version: 4.0	Financial Transaction Services (FinTS) Dokument: Anlagen
Seite: 16	Stand: 09.07.2004	Kapitel: Berechnung der Prüfziffer für interne Zuordnungsdaten (Kunden-Referenznummer)

## IV.1 Rechengang

Die internen Zuordnungsdaten (Kunden-Referenznummer) bestehen aus 12 Ziffern und einer einstelligen Prüfziffer, bilden also eine 13stellige Zeichenkette. Diese Kette wird Zeichen für Zeichen von links nach rechts verarbeitet.

Mit dem Index  $j = 1..n$  (wobei  $n$  die Anzahl der Zeichen in der Kette einschließlich Prüfziffer ist) und mit dem Anfangswert  $P_1 = M$  für  $j = 1$  berechnet man

$$S_j = P_j I_{(M+1)} + a_{(n-j+1)}$$

$$P_{(j+1)} = S_j I_M \times 2$$

Dabei ist

$I_M$  der Rest nach Division durch  $M$ ; falls dieser gleich Null ist, ist statt dessen Wert  $M$  einzusetzen.

$I_{(M+1)}$  der Rest nach Division durch  $(M+1)$ ; hier wird der Rest niemals gleich Null

$a_{(n-j+1)}$  der Zeichenwert

Bei der Prüfung gilt die Kette als richtig, wenn  $S_n = 1 \pmod{M}$  ist.

Zur Berechnung des Prüfzeichens wird  $a_1$  so gewählt, dass  $P_n I_{(M+1)} + a_1 = 1 \pmod{M}$  ist. Mit dem für  $a_1$  gefundenen Wert werden die internen Zuordnungsdaten (Kunden-Referenznummer) ergänzt.

Financial Transaction Services (FinTS) Dokument: Anlagen	Version: 4.0	Kapitel: IV
Kapitel: Berechnung der Prüfziffer für interne Zuordnungsdaten (Kunden-Referenznummer)	Stand: 09.07.2004	Seite: 17

## IV.2 Beispiel

Die internen Zuordnungsdaten (Kunden-Referenznummer) lauten 100845456115. Sie sind am rechten Ende zu ergänzen durch die Prüfziffer nach DIN ISO 7064, MOD 11,10.

### ♦ Rechnung

Schritt	Über- tragenes Produkt		nächster Zeichen- wert	Zwischen- summe	Zwischen- summe (mod 10) x 2 = Produkt	Produkt (mod 11) Ü- bertrag
j	$P_{j 11}$	+	$a_{(n-j+1)}$	$= S_j$	$S_{j 10} \times 2 = P_{(j+1)}$	$P_{(j+1) 11}$
1			2		3	4
1	10	+	1	= 11	$1 \times 2 = 2$	2
2	2	+	0	= 2	$2 \times 2 = 4$	4
3	4	+	0	= 4	$4 \times 2 = 8$	8
4	8	+	8	= 16	$6 \times 2 = 12$	1
5	1	+	4	= 5	$5 \times 2 = 10$	10
6	10	+	5	= 15	$5 \times 2 = 10$	10
7	10	+	4	= 14	$4 \times 2 = 8$	8
8	8	+	5	= 13	$3 \times 2 = 6$	6
9	6	+	6	= 12	$2 \times 2 = 4$	4
10	4	+	1	= 5	$5 \times 2 = 10$	10
11	10	+	1	= 11	$1 \times 2 = 2$	2
12	2	+	5	= 7	$7 \times 2 = 14$	3
13	3	+	8	= 1		
				(mod 10)		

Die gesuchte Prüfziffer ist 8.

### ♦ Erläuterungen

Der Ausgangswert, auf den im 1. Schritt der 1. Zeichenwert addiert wird, ist immer 10.

Zwischensumme (mod 10): Das Ergebnis der Rechenoperation in Sp. 2 wird durch 10 dividiert; der Divisionsrest (Einerstelle des Ergebnisses) ergibt die Zwischensumme  $S_{j|10}$ .

Ist dieser Wert = 0, ist statt dessen der Wert 10 zu setzen.

Produkt (mod 11): Das Produkt in Sp. 3 wird durch 11 dividiert; der Divisionsrest ergibt den nächsten Berechnungsschritt.

Prüfziffer: Im letzten Berechnungsschritt ist der Übertrag auf den Wert 11 (= 1 (mod 10)) zu ergänzen. Der gefundene Zeichenwert ist die Prüfziffer. Ist der Übertrag aus Schritt 12 jedoch = 1, so ist die Prüfziffer = 0.

Kapitel: V	Version: 4.0	Financial Transaction Services (FinTS) Dokument: Anlagen
Seite: 18	Stand: 09.07.2004	Kapitel: LÄNDERKENNZEICHEN UND WÄHRUNGSCODES Abschnitt:

## V. LÄNDERKENNZEICHEN UND WÄHRUNGSCODES

Nachfolgend sind für ausgewählte Länder jeweils der Ländercode laut ISO 3166-1 sowie der Währungscode und die Anzahl der Währungsnachkommastellen laut ISO 4217 aufgelistet:

Ländername	Ländercode (numerisch)	Ländercode (Alpha-2)	Währungs- code	Nachkomma- stellen
Belgien	056	BE	EUR	2
Bulgarien	100	BG	BGL	2
Dänemark	208	DK	DKK	2
Deutschland	280 <sup>2</sup>	DE	EUR	2
Finnland	246	FI	EUR	2
Frankreich	250	FR	EUR	2
Griechenland	300	GR	EUR	2
Großbritannien	826	GB	GBP	2
Irland	372	IE	EUR	2
Island	352	IS	ISK	2
Italien	380	IT	EUR	2
Japan	392	JP	JPY	0
Kanada	124	CA	CAD	2
Kroatien	191	HR	HRK	2
Liechtenstein	438	LI	CHF	2
Luxemburg	442	LU	EUR	2
Niederlande	528	NL	EUR	2
Norwegen	578	NO	NOK	2
Österreich	040	AT	EUR	2
Polen	616	PL	PLN	2
Portugal	620	PT	EUR	2
Rumänien	642	RO	ROL	2
Russische Föderation	643	RU	RUR	2
Schweden	752	SE	SEK	2
Schweiz	756	CH	CHF	2
Slowakei	703	SK	SKK	2
Slowenien	705	SI	SIT	2
Spanien	724	ES	EUR	2
Tschechien	203	CZ	CZK	2
Türkei	792	TR	TRL	2
Ungarn	348	HU	HUF	2
USA	840	US	USD	2

Euro	978	EU	EUR	2
------	-----	----	-----	---

<sup>2</sup> Der neue Code 276 wird derzeit noch nicht verwendet, da der Code 280 im Kreditgewerbe gebräuchlicher ist.

Financial Transaction Services (FinTS) Dokument: Anlagen	Version: 4.0	Kapitel: VI
Kapitel: Europäische Kontenadressierung Abschnitt:	Stand: 09.07.2004	Seite: 19

## VI. EUROPÄISCHE KONTENADRESSIERUNG

Die DEG „Kontoverbindung“ (s. Kap. II.5.3.3) ist für wichtige europäische Zielländer wie folgt zu belegen:<sup>3</sup>

### Belgien:

Länderkennzeichen: 056

Kreditinstitutscode: Das Feld wird nicht belegt (Der Bank-Code ist fester Bestandteil der Kontonummer).

Konto-/Depotnummer: Es ist die gesamte Ziffernfolge (genau 12-stellig) einzutragen.

3 n <sup>4</sup>	7 n	2 n
Bank-Code	No. Compte oder Rekeningnr.	Check Digit

### Dänemark:

Länderkennzeichen: 208

Kreditinstitutscode: Das Feld wird mit dem S.W.I.F.T.-Code belegt.

8 bzw. 11 an
S.W.I.F.T.-Code

Konto-/Depotnummer: Der Bank-Code ist fester Bestandteil der Kontonummer. Es ist die gesamte Ziffernfolge (max. 14-stellig) einzutragen.

4 n	max. 9 n	1
Bank-Code	Konto	Check digit

### Deutschland:

Länderkennzeichen: 280

Kreditinstitutscode: Das Feld wird mit der Bankleitzahl belegt.

8 n
Bankleitzahl

Konto-/Depotnummer: Der Bank-Code ist kein fester Bestandteil der Kontonummer. Es ist die Kontonummer einzutragen.

10 n
Kontonummer

<sup>3</sup> vgl. „Register of European Account Numbers“, ECBS Technical Report TR 201, Version 2.1, September 1999 (<http://www.ecbs.org/download/tr201v2.1.pdf>)

<sup>4</sup> Die Formatangabe gibt Länge und Datentyp des jeweiligen Feldes/Subfeldes an (n = numerisch; an = alphanumerisch)

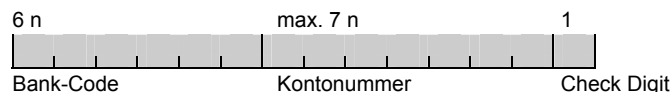
Kapitel: VI	Version: 4.0	Financial Transaction Services (FinTS) Dokument: Anlagen
Seite: 20	Stand: 09.07.2004	Kapitel: Europäische Kontenadressierung Abschnitt:

### **Finnland:**

Länderkennzeichen: 246

Kreditinstitutscode: Das Feld wird nicht belegt (Der Bank-Code ist fester Bestandteil der Kontonummer).

Konto-/Depotnummer: Es ist die gesamte Ziffernfolge (max. 14-stellig) einzutragen.

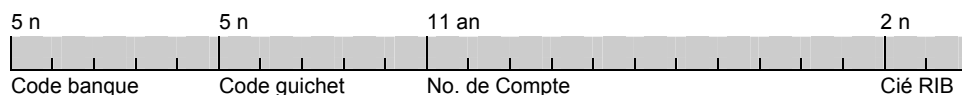


### **Frankreich:**

Länderkennzeichen: 250

Kreditinstitutscode: Das Feld wird nicht belegt.

Konto-/Depotnummer: Der RIB-Code ist eine Kombination aus Bank-Code und Kontonummer. Es ist die gesamte Ziffernfolge (genau 23 Stellen) einzutragen.



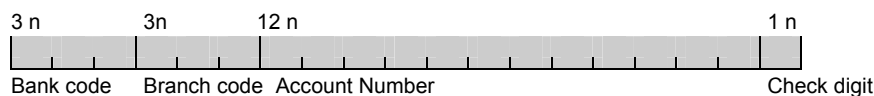
### **Griechenland:**

Länderkennzeichen: 300

Kreditinstitutscode: Das Feld wird mit dem S.W.I.F.T.-Code belegt.



Konto-/Depotnummer: Der Bank-Code ist fester Bestandteil der Kontonummer. Es ist die gesamte Ziffernfolge (genau 19 Zeichen) einzutragen.



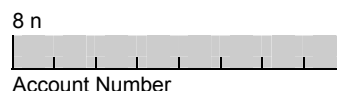
### **Großbritannien:**

Länderkennzeichen: 826

Kreditinstitutscode: Das Feld wird mit dem Sort-Code belegt.



Konto-/Depotnummer: Es ist die Kontonummer einzutragen.





Financial Transaction Services (FinTS) Dokument: Anlagen	Version: 4.0	Kapitel: VI
Kapitel: Europäische Kontenadressierung Abschnitt:	Stand: 09.07.2004	Seite: 21

### Irland:

Länderkennzeichen: 372

Kreditinstitutscode: Das Feld wird mit dem Sort-Code belegt.

6 n

Sort-Code

Konto-/Depotnummer: Es ist die Kontonummer einzutragen.

8 n

Account Number

### Island:

Länderkennzeichen: 352

Kreditinstitutscode: Das Feld wird mit dem Bank-Code belegt. Alternativ kann auch der S.W.I.F.T.-Code angegeben werden.

4 n

Bankanúmer

Konto-/Depotnummer: Es ist die Kontonummer einzutragen.

18 n

Reikningsnúmer

### Italien:

Länderkennzeichen: 380

Kreditinstitutscode: Das Feld wird mit dem S.W.I.F.T.-Code belegt.

8- bzw. 11 an

S.W.I.F.T.-Code

Konto-/Depotnummer: Der Coordinata Bancaria ist eine Kombination aus Bank-Code und Kontonummer. Es ist die gesamte Ziffernfolge (genau 23 Stellen) einzutragen.

1 a 5 n

5 n

max. 12 x

CIN ABI Code

CAB Code

Numero di Conto

### Liechtenstein:

Länderkennzeichen: 438

Kreditinstitutscode: Das Feld wird mit dem Bank-Code („SIC-Code“) belegt. Alternativ kann auch der S.W.I.F.T.-Code angegeben werden.

max. 5 an

SIC-Code



Financial Transaction Services (FinTS) Dokument: Anlagen	Version: 4.0	Kapitel: VI
Kapitel: Europäische Kontenadressierung Abschnitt:	Stand: 09.07.2004	Seite: 23

5 n

Bankleitzahl

Konto-/Depotnummer: Es ist die Kontonummer einzutragen.

11 n

Kontonummer

### Portugal:

Länderkennzeichen: 620

Kreditinstitutscode: Das Feld wird nicht belegt (Der Bank-Code ist ein fester Bestandteil der Kontonummer).

Konto-/Depotnummer: Es ist die gesamte Ziffernfolge (insgesamt max. 21 Stellen) einzutragen.

4 n

National Bank  
Code

4 n

Bank Branch  
Code

11 n

Kontonummer

2 n

Check  
Digit

### Schweden:

Länderkennzeichen: 752

Kreditinstitutscode: Das Feld wird nicht belegt (Der Bank-Code ist ein fester Bestandteil der Kontonummer).

Konto-/Depotnummer: Es ist die Kontonummer (insgesamt max. 15-stellig, meist 11-stellig) anzugeben.

4 n

Bank-Code

6 n

Kontonummer

1 n

Check Digit

### Schweiz:

Länderkennzeichen: 756

Kreditinstitutscode: Der Bank-Code ist kein fester Bestandteil der Kontonummer. Alternativ kann auch der S.W.I.F.T.-Code angegeben werden.

max. 5 n

Clearingnummer

Konto-/Depotnummer: Es ist die Kontonummer einzutragen.

max. 16 an

Kontonummer

### Spanien:

Länderkennzeichen: 724

Kreditinstitutscode: Das Feld wird nicht belegt (Der Bank-Code ist ein fester Bestandteil der Kontonummer).

Kapitel: VI	Version: 4.0	Financial Transaction Services (FinTS) Dokument: Anlagen
Seite: 24	Stand: 09.07.2004	Kapitel: Europäische Kontenadressierung Abschnitt:

Konto-/Depotnummer: Es ist die gesamte Ziffernfolge (genau 20-stellig) einzutragen.

4 n	4 n	2 n	10 n
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Código de entidad	Código de oficina	Dígitos de control	Número de cuenta

Financial Transaction Services (FinTS) Dokument: Anlagen	Version: 4.0	Kapitel: VII
Kapitel: Verweise auf verwendete Dokumente Abschnitt:	Stand: 09.07.2004	Seite: 25

## VII. VERWEISE AUF VERWENDETE DOKUMENTE

---

Die Verweise und weiterführende Literatur sind nachfolgend nach Themenbereichen geordnet:

### ♦ FinTS

[Formals] Financial Transaction Services (FinTS) – Formals (Grundsätzliche Festlegungen), Version 4.0 final draft 02, 02.04.2004, Zentraler Kreditausschuss

[Syntax] Financial Transaction Services (FinTS) – XML-Syntax, Version 4.0 final draft 02, 02.04.2004, Zentraler Kreditausschuss

### ♦ Allgemeines

[ISO 639-1] ISO 639-1:2002: Code for the representation of names of languages – Part 1: Alpha-2 code  
(<http://lcweb.loc.gov/standards/iso639-2/iso639jac.html>)

[ISO 3166] ISO 3166-1:1996: Code for the representation of names of countries and their subdivisions - Part 1: Country code  
(<http://www.din.de/gremien/nas/nabd/iso3166ma/> oder <http://www.unece.org/trade/locode/loc99.zip>)

[ISO 4217] ISO 4217:1995: Codes for the representation of currencies and funds

[ISO 8601] ISO 8601:2000: Data elements and interchange formats -- Information interchange -- Representation of dates and times  
(<http://www.iso.ch/markete/8601.pdf>)

[ISO 8859] ISO 8859-1:1987: Information processing - 8 bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1

[ISO 13616] ISO 13616: Banking and related services - International Bank Account Number (IBAN)

[EBS 204] International Bank Account Number (IBAN), European Banking Standard EBS 204, Version 3.2, hrsg. v. European Committee for Banking Standards, August 2003 (<http://www.ecbs.org>)

[SIG 203] IBAN: Standard Implementation Guidelines (SIG 203), hrsg. v. European Committee for Banking Standards, November 1996  
(<http://www.ecbs.org/download.html>)

### ♦ Sicherheit

[ZKA-Abkommen]

Kryptographische Verfahren des deutschen Kreditgewerbes für die Elektronische Unterschrift und für die Verschlüsselung im Rahmen

Kapitel: VII	Version: 4.0	Financial Transaction Services (FinTS) Dokument: Anlagen
Seite: 26	Stand: 09.07.2004	Kapitel: Verweise auf verwendete Dokumente Abschnitt:

der Kunde-Bank-Kommunikation

in: ZKA-Abkommen über die Datenfernübertragung zwischen Kunden und Kreditinstituten (DFÜ-Abkommen) v. 15.03.1995, Anlage 2

- [ISO 9735-5] ISO 9735-5:1999 Electronic data interchange for administration, commerce and transport - (EDIFACT) - Application level syntax rules; (Syntax version number: 4) - Part 5: Security rules for batch EDI (Authenticity; Integrity and Non-repudiation of origin)
- [ISO 9735-7] ISO 9735-7:1999 Electronic data interchange for administration, commerce and transport - (EDIFACT) - Application level syntax rules; (Syntax version number: 4) – Part 7: Security rules for batch EDI (Confidentiality)
- [ISO 9735-9] ISO 9735-9:1999 Electronic data interchange for administration, commerce and transport - (EDIFACT) - Application level syntax rules; (Syntax version number: 4) – Part 9: Security key and certificate management message (Message type - KEYMAN)
- [ISO 9796-2] ISO 9796-2:1997: Information technology - Security techniques - Digital signature scheme giving message recovery – Part 2: Mechanisms using a hash-function
- [ISO 9796-3] ISO 9796-3:2000 Information technology - Security techniques - Digital signature scheme giving message recovery – Part 3: Discrete logarithm based mechanisms
- [ISO 10116] ISO 10116:1997 Information technology Security techniques - Modes of operation for an n-bit block cipher algorithm
- [ISO 10118-2] ISO 10118-2:1994 Information technology - Security techniques - Hash functions Part 2: Hash functions using an n-bit block cipher algorithm
- [ISO 10118-3] ISO 10118-3:1998 Information technology - Security techniques - Hash functions Part 3: Dedicated hash-functions, Draft, 1997
- [ISO 10126-1] ISO 10126-1:1991: Banking - Procedures for message encipherment (wholesale) – Part 1: General principles
- [ISO 10126-2] ISO 10126-2:1991 Banking - Procedures for message encipherment (wholesale) – Part 2: DEA algorithm
- [X3.92] ANSI X3.92-1981 (R1987): Data Encryption Algorithm
- [X3.106] ANSI X3.106-1983 (R1996): Data Encryption Algorithm, Modes of operation for the
- [X9.19] ANSI X9.19-1996: Financial Institution Retail Message Authentication

Financial Transaction Services (FinTS) Dokument: Anlagen	Version: 4.0	Kapitel: VII
Kapitel: Verweise auf verwendete Dokumente Abschnitt:	Stand: 09.07.2004	Seite: 27

- [X9.23] ANSI X9.23-1995 (R1995): Financial Institution Encryption of Wholesale Financial Messages
- [CIPHER] EDIFACT Message Implementation Guidelines: Ciphred Text Message. CIPHER, SJWG; Working Draft Version, Paris September 16th 1994
- [EDIFACT SIG] EDIFACT Security Implementation Guidelines, Trade/WP.4/R.1026/Add.2, 22 February
- [KEYMAN] MIG Handbook UN/EDIFACT Message KEYMAN (proposed draft), June 30, 1995
- [RSA] R. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, vol. 21 no. 2, 1978.
- [RIPEMD] H. Dobbertin, A. Bosselaers, B. Preneel: „RIPEMD-160, a strengthened version of RIPEMD“, Fast Software Encryption - Cambridge Workshop 1996, LNCS, Band 1039, D. Gollmann, Ed., Springer-Verlag, 1996, S. 71-82  
(<http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html>)

#### ♦ Transportmedienspezifische Festlegungen

- [RFC 791] Request for Comment (RFC) 791: Internet Protocol (IP), September 1981
- [RFC 1700] Request for Comment (RFC) 1700: Assigned Numbers, Oktober 1994
- [RFC 2616] Request for Comment (RFC) 2616: Hypertext Transfer Protocol – HTTP/1.1, Juni 1999
- [RFC 821] Simple Mail Transfer Protocol
- [RFC 2045] Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
- [RFC 2046] Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types

Bezugsquelle für RFC-Dokumente: z. B. <ftp://ftp.eunet.de/pub>

#### ♦ Geschäftsvorfälle

- [Richtl. ZV] Richtlinien für einheitliche Zahlungsverkehrsvordrucke und Merkblätter für neutrale Zahlungsverkehrsvordrucke
- [SWIFT] S.W.I.F.T. User Handbook, October 1998 Standards Release

Kapitel: VII	Version: 4.0	Financial Transaction Services (FinTS) Dokument: Anlagen
Seite: 28	Stand: 09.07.2004	Kapitel: Verweise auf verwendete Dokumente Abschnitt:

- [ISO 6166] ISO 6166: International Securities Numbering System
- [ISO 9362] ISO 9362: Bank Identifier Code (BIC)
- [ISO 10383] ISO 10383: Market Identifier Code (MIC)
- [ISO 15022-1] ISO 15022-1:1999 Securities - Scheme for messages (Data Field Dictionary) - Part 1: Data field and message design rules and guidelines (<http://www.iso15022.org>)
- [ISO 15022-2] ISO 15022-2:1999 Securities - Scheme for messages (Data Field Dictionary) - Part 2: Maintenance of the Data Field Dictionary and Catalogue of Messages (<http://www.iso15022.org>)
- [TR 201] Register of European Account Numbers, Technical Report TR 201, Version 2.1, hrsg. v. European Committee for Banking Standards, September 1999 (<http://www.ecbs.org>)
- [EBS 206] International Payment Instruction (IPI), European Banking Standard EBS 206, Version 1.4, hrsg. v. European Committee for Banking Standards, November 1999 (<http://www.ecbs.org>)

#### ♦ Chipkartenspezifikation

- [ISO PIN1] ISO 9564-1, Banking – Personal Identification Number Management and Security, Part 1: PIN protection principles and techniques, DIS 1999
- [LIT 1'] Schnittstellenspezifikation für die ZKA-Chipkarte, Datenstrukturen und Kommandos, Version 4.1, 01.07.1999
- [LIT 1A] Schnittstellenspezifikation für die ec-Karte mit Chip, Dateien des MF, Version 4.2, 01.12.1999
- [LT] Schnittstellenspezifikation für die ec-Karte mit Chip, Ladeterminal, Version 3.0, 02.04.1998