# FinTS

# Financial Transaction Services

- Schnittstellenspezifikation -

## *Security*

**Sicherheitsverfahren PIN/TAN**

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 Banking-Schnittstelle (im Folgenden: Schnittstellenspezifikation) wurde im Auftrag des Zentralen Kreditausschusses entwickelt. Sie wird hiermit zur Implementation in Kunden- und Kreditinstitutssysteme freigegeben.



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

## *Versionsführung*

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

| Name | Organi-sation | Datum | Version | Dokumente | Anmerkungen |
|---|---|---|---|---|---|
| Stein | SIZ | 15.11.2002 | 3.0 | FinTS 3.0 Security – Sicherheitsverfah-ren PINTAN.doc | |
| | SIZ | 02.05.2003 | 4.0ref | FinTS_4.0_Security_PIN TAN.doc | Anpassungen für FinTS 4.0 |
| | SIZ | 19.11.2003 | 4.0 final draft 01 | FinTS_4.0_Security_PIN TAN.doc | Überarbeitungen |
| | SIZ | 02.04.2004 | 4.0 final draft 02 | FinTS_4.0_Security_PIN TAN.doc | Überarbeitungen |
| | SIZ | 09.07.2004 | 4.0 | FinTS_4.0_Security_PIN TAN.doc | Überarbeitungen |

## *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.

| lfd. Nr. | Kapitel | Kapitel-nummer | Kennung[1] | Art[2] | Beschreibung |
|---|---|---|---|---|---|
| 1 | Verfahrensbeschreibung | II.5.1 | | K | Hinweis zur Verwendung einer TAN für mehrere Aufträge |
| 2 | | II.6 | | K | Signaturpflicht für administrative Aufträge |

[1] nur zur internen Zuordnung
[2] F = Fehler; Ä = Änderung; K = Klarstellung; E = Erweiterung

# *Inhaltsverzeichnis*

# *Abbildungsverzeichnis*

# *Abkürzungen*

| Abkürzung | Bedeutung |
| --- | --- |
| BPD | Bankparameterdaten |
| C | Datenstruktur ist konditional |
| CR | Carriage-Return (Wagenrücklauf) |
| DDV | DES-DES-Verfahren |
| DE | Datenelement |
| DEG | Datenelementgruppe |
| DES | Data Encryption Standard |
| DF | Dedicated File |
| DFÜ | Synonym verwendet für "Datenkommunikation, die in Form von Filetransfer, E-Mail, Online-Nachrichtenaustausch etc. erfolgen kann |
| EF | Elementary File |
| EU | Elektronische Unterschrift; basiert auf dem asymmetrischen RSA-Verfahren |
| FinTS | Financial Transaction Services |
| GD | Gruppendatenelement |
| GDG | Gruppendatenelementgruppe |
| HBCI | Homebanking Computer Interface |
| I | Information (z. B. Schlüsselart) |
| ID | Identifikationsmerkmal (Nummer oder alphanumerischer Code) |
| ISO | International Organisation for Standardisation |
| LF | Line-Feed (neue Zeile) |
| M | Datenstruktur muss vorhanden sein und ist inhaltlich korrekt zu füllen |
| MAC | Message Authentication Code; Symmetrisches Verfahren zur Erzeugung einer elektronischen Signatur (derzeit für die ZKA-Chipkarte eingesetzt) |
| MIME | Multipurpose Internet Mail Extensions |
| N | Nachricht |
| N | Nicht erlaubt (not allowed) (Datenstruktur darf nicht vorhanden sein) |
| O | Datenstruktur ist optional |
| PIN | Private Identifikationsnummer |
| RDH | RSA-DES-Hybridverfahren |
| RFC | Request for Comment |
| RSA | Asymmetrischer Algorithmus für die elektronische Unterschrift (EU) (vgl. MAC), benannt nach den Erfindern Rivest, Shamir und Adleman. |
| SEG | Segment |
| SEQ | Sequenznummer |
| SF | Segmentfolge |

| Abkürzung | Bedeutung |
|---|---|
| SSL | Secure Socket Layer |
| T | Transaktion (z. B. Schlüsselart) |
| TAN | Transaktionsnummer |
| UPD | User-Parameterdaten |
| ZKA | Zentraler Kreditausschuss |

## *Literaturhinweise*

[Formals] Financial Transaction Services (FinTS) – Formals (Allgemeine Festlegungen für multibankfähige Online-Verfahren der deutschen Kreditwirtschaft), Version 4.0 final draft 02, 02.04.2004, Zentraler Kreditausschuss

[HBCI] Financial Transaction Services (FinTS) – Security (Sicherheitsverfahren HBCI), Version 4.0 final draft 02, 02.04.2004, Zentraler Kreditausschuss

[Messages] Financial Transaction Services (FinTS) – Messages (Multibankfähige Geschäftsvorfälle), 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

[ZKA-Dialog] PC-Btx-Dialog („ZKA-Dialog“), Zentraler Kreditausschuss, 03.09.1998 http://www.fints.de/download/ZKA-Dialog_1999-01-01.pdf

# I. EINLEITUNG

In dieser Spezifikation wird ein multibankfähiges Protokoll für das Sicherheitsverfahren PIN/TAN beschrieben. Dieses ersetzt den bisher über Btx abgewickelten „ZKA-Dialog“ [ZKA-Dialog].

Dieses Sicherheitsverfahren kann in multibankfähigen Online-Banking-Verfahren der deutschen Kreditwirtschaft eingesetzt werden. Informationen bzgl. Nachrichtenaufbau und Kommunikationsablauf sind dem Dokument [Formals] zu entnehmen.

Um ein möglichst hohes Maß an Synergie nutzen zu können, wird für die Kommunikation zwischen Kundenprodukt und Kreditinstitut weitestgehend auf der FinTS-Spezifikation in der Version 4.0 aufgesetzt, insbesondere bzgl. Syntax, Datenformaten und Abläufen. Sofern nicht anders vermerkt gelten für den Nachrichtenaufbau, Kommunikationsablauf etc. die dort getroffenen Regelungen. Dieses Dokument beschreibt daher nur die für das PIN/TAN-Verfahren abweichenden Festlegungen.

Die deutsche Kreditwirtschaft forciert seit Jahren das Online-Banking mit FinTS (Financial Transaction Services). Mittlerweile bietet die überwiegende Zahl der Kreditinstitute ihren Benutzern dieses Verfahren an. FinTS konkurriert damit mit einigen anderen Verfahren, die in der Regel PIN und TAN für die Authentisierung und Autorisierung des Benutzers verwenden:

- T-Online Classic („Btx-CEPT-Banking“)
- Internet-Browserbanking
- Gateways verschiedener Hersteller als Zugangsrechner für bestimmte Kundenprodukte

Aus verschiedenen Gründen bieten die Kreditinstitute diese Verfahren oft parallel an. Die Einführung eines PIN/TAN-Protokolls auf Basis der FinTS-Syntax bietet somit die Möglichkeit, sämtliche Online-Banking-Verfahren über eine einheitliche Plattform abzuwickeln (s. Abbildung 1 und Abbildung 2).

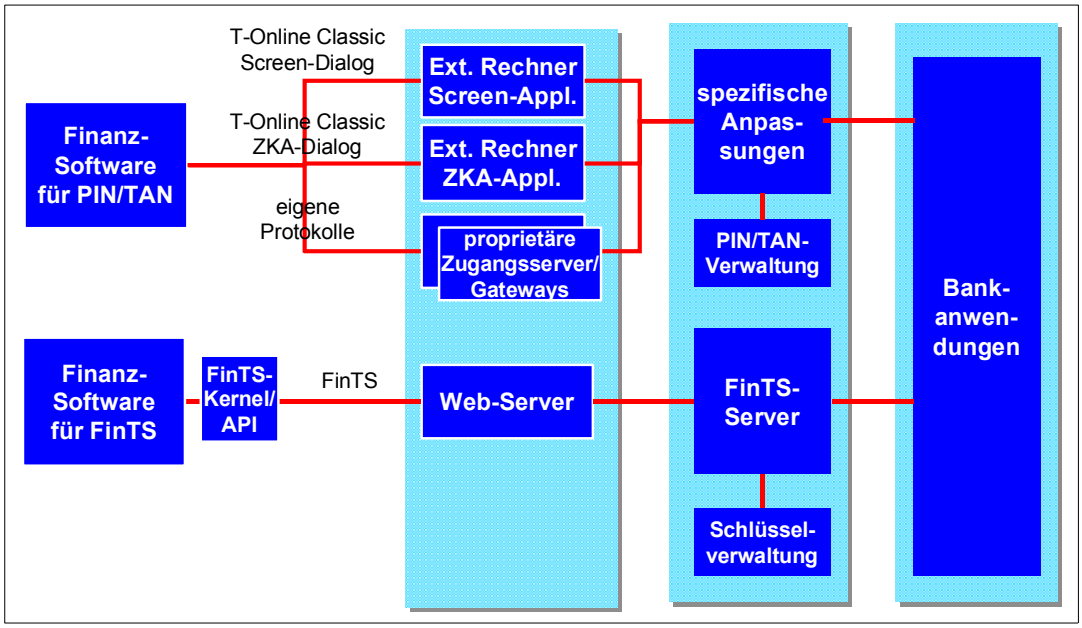


*Abbildung 1: Online-Banking mit PIN/TAN traditionell und FinTS*

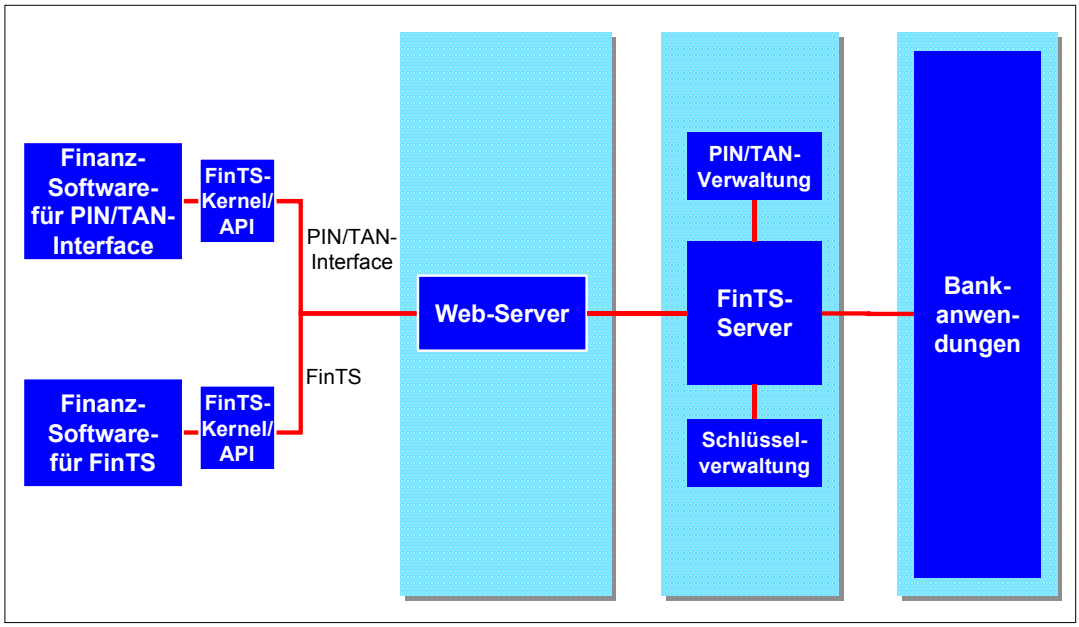


*Abbildung 2: Online-Banking mit PIN/TAN und FinTS*

Während FinTS seine Stärken derzeit insbesondere in der hohen Sicherheit hat, ist als Vorteil des PIN/TAN-Verfahrens beispielsweise die höhere Mobilität zu sehen. Dies bedeutet, der Benutzer kann Online-Banking ohne zusätzliche Infrastruktur betreiben. PIN/TAN ist somit eine gute Lösung für die eilige Überweisung aus dem Büro, während FinTS für die umfassende Kontenverwaltung mit einem Offline-Kundenprodukt in Frage kommt.

Die Kreditinstitute unterstützen daher oft beide Verfahren parallel. Dies führt dazu, dass der Benutzer zwar aus mehreren Alternativen das für ihn bestgeeignete Verfahren auswählen kann, für die Kreditinstitute hiermit jedoch hohe Aufwendungen verbunden sind, z. B. durch

- Pflege unterschiedlicher Schnittstellen
- inkompatible Systeme oftmals unterschiedlicher Hersteller
- redundante Stammdatenhaltung

Verschärfend kommt hinzu, dass der CEPT-Dialog über T-Online eine auslaufende Technologie ist und T-Online aus diesem Grund die Preise für die Anbindung externer Rechner über Datex-P ab Anfang 2002 stark erhöht hat. Die Kreditinstitute suchen daher nach preisgünstigen aber gleichzeitig zukunftsweisenden Alternativen.

Die Lösung verfolgt als primären Zweck das Homebanking mit Offline-Finanzsoftwareprodukten. Bei HTML-basierten Browser-Banking-Lösungen ist der Einsatz des PIN/TAN-Interfaces zum einen nicht erforderlich, da hierbei keine Multibankfähigkeit benötigt wird, und zum anderen technisch kaum realisierbar, da aus der Anwendung ein FinTS-Kernel angesprochen werden muss.

Ob ein Kreditinstitut das PIN/TAN-Interface anbietet, erkennt das Kundenprodukt am Vorhandensein des Segments Parameterdaten PIN/TAN bzw. des Kommunikationsdienstes HTTPS in den Bankparameterdaten (siehe [Formals], Abschnitt *IV.2.3 Sicherheitsverfahren*).

Grundsätzlich können mit dem Sicherheitsverfahren PIN/TAN alle im Dokument [Messages] aufgeführten Geschäftsvorfälle verwendet werden. Dies gilt auch für

verbandsindividuelle Erweiterungen. Welche Geschäftsvorfälle konkret zulässig sind, teilt das Kreditinstitut im Segment Parameterdaten PIN/TAN (siehe *II.4 Bankparameterdaten zum PIN/TAN-Verfahren*) mit.

Da im PIN/TAN-Interface aufgrund der nicht vorhandenen kryptographischen Verfahren auf Protokollebene keine Verschlüsselung zum Einsatz kommen kann, wird ausschließlich SSL auf Transportebene verwendet. Eine Verschlüsselung auf FinTS-Protokollebene entfällt komplett. Die Lösung verbindet damit die Sicherheit eines Einmalpassworts (TAN) mit der in SSL bewährten 128 bit-Transportverschlüsselung.

Es wird eine möglichst breite Unterstützung dieser Spezifikation auf Seite der Kundenprodukte und Kreditinstitute angestrebt.

Die Vorteile des PIN/TAN-Interfaces:

- Migration aller Onlinebanking-Verfahren auf Internet-Kommunikation und somit Möglichkeit zum Verzicht auf T-Online
- Im Vergleich zu T-Online/CEPT kostengünstige Homebankinglösung, da bankseitig keine Datex-P-Gebühren anfallen
- Abwicklung aller Onlinebanking-Verfahren (PIN/TAN und FinTS) über eine einheitliche Plattform
- Ersatz proprietärer, inkompatibler Herstellerlösungen durch eine standardisierte Lösung aus einer Hand
- Auch für Nicht-T-Online-Nutzer nutzbar
- Verfügbarkeit aller FinTS-Geschäftsvorfälle auch für PIN/TAN-Nutzer
- Die Anpassung bestehender FinTS-Kundenprodukte ist mit Hilfe eines durch das PIN/TAN-Interface erweiterten FinTS-Kernels problemlos möglich.
- Einheitliche Stammdatenhaltung für alle Onlinebanking-Verfahren
- Einheitliche Anbindung der Backend-Anwendungen
- Benutzerauthentisierung und -autorisierung an einer zentralen Stelle
- Erstmalige Standardisierung der Geschäftsvorfälle für das PIN/TAN-Management

# II. VERFAHRENSBESCHREIBUNG

## II.1 Allgemeines

Es gelten die in [Formals] aufgeführten Formate und Belegungsrichtlinien.

Ergänzend hierzu gilt:

- PIN und TAN werden in die DEG PIN/TAN-Signatur eingestellt. Diese ersetzt die bei HBCI-Sicherheitsverfahren einzustellenden Signaturen nach XML-Signature-Standard.
- Für die Rückmeldungen wurden neue Codes definiert (siehe *II.2 Erweiterung der Rückmeldungscodes*)
- Wie beim DDV-Verfahren sind die Anforderung von Kreditinstitutsschlüsseln sowie Schlüsselsperr- und Schlüsseländerungsnachrichten verboten.
- Die Bankparameterdaten enthalten ein Parametersegment, welches die PIN/TAN-spezifischen Informationen des Kreditinstituts enthält.
- Die für den Benutzer zugelassenen Geschäftsvorfälle für das PIN/TAN-Management sind ihm über dessen UPD mitzuteilen.
- Diejenigen FinTS-Benutzer, die das PIN/TAN-Verfahren verwenden, können nicht auf FinTS-Protokollebene verschlüsseln. Es ist allein eine SSL-Transportverschlüsselung möglich. Für den Boten einer Nachricht bedeutet dies, dass seine Botenverschlüsselung durch eine SSL-Transportverschlüsselung ersetzt werden kann. Für den Herausgeber eines Auftragsteils bedeutet dies jedoch, dass eine gesonderte Verschlüsselung des Auftragsteiles bei Verwendung des PIN/TAN-Verfahrens nicht möglich ist. Komprimierung ist jedoch auf beiden Ebenen möglich.
- Als Kommunikationsdienst ist HTTPS laut den Vorgaben des `CommSettings_Reply`-Segmentes aus den BPD zu verwenden (siehe [FORMALS], Abschnitt *IV. BANKPARAMETERDATEN (BPD)*).
- Das in diesem Dokument beschriebene Verfahren wird auf Syntaxebene als „PIN/TAN-Verfahren, Variante 1.1“ bezeichnet. Zukünftige andere Parametrisierungen oder Modifikationen des Verfahrens müssen eine andere eindeutige Variantenbezeichnung erhalten, um die Multibankfähigkeit der Produkte zu gewährleisten.

Gemäß §7 der „Bedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN“ dürfen sowohl die PIN als auch TANs nicht elektronisch im Kundenprodukt gespeichert werden.

# II.2 Erweiterung der Rückmeldungscodes

Bei Verwendung des PIN/TAN-Verfahrens können spezielle Rückmeldecodes vom Kreditinstitut zurückgemeldet werden, die rein PIN/TAN-spezifisch sind und nicht direkt mit dem zugehörigen Geschäftsvorfall in Verbindung stehen. Es handelt sich hierbei um die folgenden Codes:

- **Erfolgsmeldungen**

| Code | Beispiel für Rückmeldungstext |
|---|---|
| 0010 | Auftrag entgegengenommen |
| 0020 | TAN-Liste Nr. xxx aktiviert |
| 0020 | PIN-Sperre erfolgreich |
| 0020 | PIN-Sperre aufgehoben |
| 0020 | PIN geändert |
| 0020 | TAN-Liste gesperrt |
| 0900 | TAN gültig |
| 0901 | PIN gültig |

- **Warnungen und Hinweise**

| Code | Beispiel für Rückmeldungstext |
|---|---|
| 3910 | TAN wurde nicht verbraucht |
| 3911 | Bitte neue TAN-Liste aktivieren |
| 3912 | neue TAN-Liste wird automatisch verschickt |
| 3913 | TAN wurde verbraucht |
| 3914 | neue TAN-Liste aktivieren |
| 3915 | neue TAN-Liste aktiviert |
| 3916 | PIN muss wegen erstmaliger Anmeldung zwangsweise geändert werden |
| 3917 | Alte TAN-Liste ist infolge der Aktivierung einer neuen TAN-Liste ungültig |
| 3931 | PIN gesperrt. Entsperren mit GV „PIN-Sperre aufheben“ möglich |

- **Fehlermeldungen**

| Code | Beispiel für Rückmeldungstext |
|---|---|
| 9931 | Teilnehmersperre durchgeführt, Entsperren nur durch Kreditinstitut |
| 9941 | TAN ungültig |
| 9942 | PIN ungültig |
| 9942 | neue PIN ungültig |
| 9943 | TAN bereits verbraucht |

# II.3 Bankfachliche Anforderungen

Es gelten die in [HBCI], Abschnitt *II.4 Bankfachliche Anforderungen* aufgeführten Regelungen. Abweichend hierzu gilt:

- **Zu signierende Nachrichten**

  Wie auch beim Sicherheitsverfahren HBCI ist die Signatur von Kreditinstitutsnachrichten optional. Da der Benutzer in seiner Auftragsnachricht das anzuwendende Signaturverfahren vorgibt, darf das Kreditinstitut jedoch nicht mit einem HBCI-Sicherheitsverfahren antworten. Es sendet daher ein entsprechendes Segment Antwort auf eine PIN/TAN-Signatur zurück (siehe [Syntax]).

- **Doppeleinreichungskontrolle**

  Im PIN/TAN-Verfahren werden keine Signatur-IDs benötigt, da hier die TAN deren Aufgabe übernimmt und durch sie eine Doppeleinreichung verhindert wird.

# II.4 Bankparameterdaten zum PIN/TAN-Verfahren

Realisierung Kreditinstitut: verpflichtend, falls Geschäftsvorfälle mit PIN/TAN-Absicherung angeboten werden
Realisierung Kundenprodukt: optional

Für die Verwendung des PIN/TAN-Verfahrens müssen dem Kundenprodukt spezielle Daten im Rahmen der BPD-Segmentfolge übermittelt werden. So ist beispielsweise anzugeben, welche Geschäftsvorfälle über PIN/TAN abgesichert werden dürfen und für welche davon eine TAN erforderlich ist. Des Weiteren werden hier Längenangaben für PIN und TAN sowie die kreditinstitutsspezifischen Belegungsvorschriften für Benutzerkennungs- und Kunden-ID-Felder in Textform übermittelt.

Hierfür existiert das Segment Parameterdaten PIN/TAN, welches die oben beschriebenen Daten aufnehmen kann. Die hier aufgeführten Geschäftsvorfälle dürfen vom Benutzer in über PIN/TAN abgesicherte Nachrichten eingestellt werden, sofern sie in den BPD und UPD als generell erlaubt hinterlegt sind. Alle übrigen Geschäftsvorfälle können mit dem PIN/TAN-Interface nicht verwendet werden.

Sollen die in [Formals], Abschnitt *III.8 Verteilte Signaturen* beschriebenen Abläufe auch mit dem PIN/TAN-Verfahren möglich sein, so müssen die zugehörigen Geschäftsvorfälle für die Abwicklung verteilter Signaturen im Segment Parameterdaten PIN/TAN hinterlegt sein. Auch die Geschäftsvorfälle, die verteilt signiert werden sollen, müssen dort hinterlegt sein.

# II.5 Sicherheitstechnische Abläufe

Bei Verwendung des PIN/TAN-Verfahrens sind alternativ zu den in [HBCI] beschriebenen Signatur-Segmenten andere Segmente in die Nachricht einzustellen, die die für das PIN/TAN-Verfahren notwendigen Daten aufnehmen können. In einer Benutzernachricht ist dies ein Segment PIN/TAN-Signatur und in einer Kreditinstitutsnachricht ein Segment Antwort auf eine PIN/TAN-Signatur (siehe auch [Syntax]).

## II.5.1 PIN/TAN-Signatur

Analog zu den in Kapitel [HBCI], Abschnitt *II.5.1 Signatur-Segment* beschriebenen Signaturen lassen sich die in PIN/TAN-Signatur-Segmenten enthaltenen Informationen in allgemeine und verfahrensspezifische Informationen aufteilen:

Zu den allgemeinen Informationen gehören:

- Rolle des Signierenden
- Zeitstempel

Zu den für PIN/TAN-spezifischen Informationen gehören:

- Kreditinstitutskennung
- Benutzerkennung
- Kundensystemkennung
- PIN (optional)
- TANs (optional; nur in Benutzernachrichten zulässig)
- Referenzen auf die über TAN abzusichernden Teile der FinTS-Nachricht

♦ **Belegungsrichtlinien**

**Rolle des Signierenden**

Es gelten die gleichen Regeln wie in [HBCI], Abschnitt *II.5.1 Signatur-Segment* beschrieben.

**Kundensystemkennung**

Die Kundensystemkennung ist für das PIN/TAN-Verfahren optional. Sie kann verwendet werden, um eine eindeutige Identifizierung eines Dialogs im Rahmen der Synchronisierung der letzten Nachrichtennummer zu ermöglichen (siehe dazu Hinweistext in [Formals], Abschnitt *III.3 Synchronisierung*). Eine Kundensystemkennung kann wie im Sicherheitsverfahren HBCI mit einer Synchronisierungsnachricht angefordert werden.

**TAN und Referenz**

Zu jeder TAN ist in der Signatur eine Referenz enthalten. Die Referenz bezeichnet denjenigen Teil der Nachricht, auf den sich die TAN bezieht.

Bei der Verwendung der PIN/TAN-Signatur als Botensignatur bezieht sich die PIN implizit auf die gesamte Nachricht. Wenn eine TAN angegeben ist,

muss sie auf den kompletten Nachrichtenkörper mit allen Aufträgen bezogen sein.

Bei einer Verwendung als Auftragssignatur bezieht sich die PIN implizit auf alle Aufträge des Auftragsteils, die TANs müssen jeweils einem Auftrag des Auftragsteils zugeordnet sein.

Falls mehrere Aufträge in einer Nachricht transportiert werden, ist bei der Verwendung von TANs Folgendes zu bedenken:

Wenn nicht erwünscht ist, dass mehrere Aufträge mit derselben TAN versehen werden, ist die Angabe einer TAN in der Botensignatur nicht sinnvoll, denn diese bezieht sich per Definition auf alle enthaltenen Aufträge. Statt dessen werden die TANs im Rahmen einer oder mehrerer Auftragssignaturen angegeben.

Ist hingegen gewollt, dass mehrere Aufträge mit derselben TAN versehen werden, so besteht entweder die Möglichkeit, die TAN in der Botensignatur anzugeben und somit alle Aufträge mit dieser TAN zu signieren, oder aber in einer oder mehreren Auftragssignaturen die gleiche TAN mit Referenzen auf unterschiedliche Aufträge anzugeben und somit gezielt bestimmte Aufträge mit derselben TAN zu versehen.

## II.5.2 Antwort auf eine PIN/TAN-Signatur

Mit dem Segment Antwort auf eine PIN/TAN-Signatur können vom Kreditinstitut PIN und TANs bestätigt und optional Bestätigungsnummern für verbrauchte TANs zurück gemeldet werden.

- PIN (optional)
- optional Paare aus TAN und zugehöriger BEN (Bestätigungsnummer, optional)

♦ **Belegungsrichtlinien**

**PIN**

Hier kann die PIN aus der PIN/TAN-Signatur zurückgespiegelt werden.

**TAN-Verbrauchsbestätigung**

Das Kreditinstitut kann den Verbrauch der TAN zurückmelden. Optional ist die Zuordnung einer Bestätigungsnummer (BEN) möglich. Ein BPD-Parameter gibt an, ob die Verbrauchsbestätigung unterstützt wird.

Da das Kreditinstitut bei Auftragssignaturen die Antwortliste grundsätzlich nur für den Auftragsüberbringer signiert (vgl.

[Formals], Abschnitt *II.10 Kreditinstitutsnachrichten allgemein*), können auch nur für diesen TAN-Verbrauchsbestätigungen geliefert werden, nicht für eventuell vorhandene weitere Signierende.

### II.5.3 Verschlüsselung im PIN/TAN-Verfahren

Im PIN/TAN-Verfahren ist eine Verschlüsselung nach kryptographischen Verfahren aus [HBCI] nicht möglich. Stattdessen ist zwischen Benutzer und Kreditinstitut beim Nachrichtentransport eine Transportverschlüsselung einzusetzen, um so den Inhalt der Nachrichten gegenüber Dritten zu schützen.

Es ist zu beachten, dass die zwischen Benutzer und Kreditinstitut ausgetauschten Nachrichten aus FinTS-Protokollsicht unverschlüsselt sind, obwohl eine personalisierte Kommunikation stattfindet. Dass die Nachrichten bei ihrem Transport transportverschlüsselt waren, kann ihnen nicht angesehen werden. Dennoch darf dies nicht zu einer Ablehnung der Nachrichten führen. Vielmehr ist eine unverschlüsselte Nachricht, die über einen transportverschlüsselten Kanal das Kundensystem bzw. das Kreditinstitut erreicht, immer wie eine Botenverschlüsselte Nachricht zu betrachten.

### II.5.4 Komprimierung im PIN/TAN-Verfahren

Eine Komprimierung ist auch im PIN/TAN-Verfahren möglich, dafür werden die gleichen Mechanismen eingesetzt wie bei Komprimierung in Kombination mit Sicherheitsmechanismen nach [HBCI].

## II.6 PIN/TAN-Management

Alle Geschäftsvorfälle zum PIN/TAN-Management enthalten explizit die Angabe eines Benutzers. Bei direkter Kommunikation eines Kunden mit dem Kreditinstitut muss mindestens eine PIN/TAN-Signatur dieses Benutzers als Herausgebersignatur (*II.5.1 PIN/TAN-Signatur* mit Rolle ISS) vorhanden sein, die sich auf diesen Auftrag bezieht. Die PIN ist dabei zwingend erforderlich, falls zusätzlich eine TAN verlangt wird, ist dies in der Beschreibung des Geschäftsvorfalls vermerkt. Folglich können die Aufträge ausschließlich in einem personalisierten Dialog eingereicht werden. Die Herausgebersignatur kann als Boten- oder als Auftragssignatur ausgeführt sein, weitere zusätzliche Signaturen sind möglich. Soll ein Intermediär einen solchen Auftrag im Namen des Benutzers einreichen (siehe [Formals], Abschnitt *II.3.2 Kommunikation über Intermediär*, Szenario A), signiert er selbst als Herausgeber. In diesem Fall muss der Intermediär – wie auch bei normalen Transaktions- und Abholaufträgen – die Verfügungsberechtigung für diesen administrativen Auftrag besitzen.

Da diese Geschäftsvorfälle in UPD und BPD aufgeführt sind (vgl. auch [Formals], Abschnitt *V. USER-PARAMETERDATEN (UPD)*, [Formals], Abschnitt *IV. BANKPARAMETERDATEN (BPD)*), kann das Kreditinstitut prinzipiell eine minimale Signaturanzahl von ‚0' für einen Geschäftsvorfall vorgeben. Die o.g. Forderung zur Herausgebersignatur gilt jedoch in jedem Fall. Ein Kundenprodukt muss also für diese administrativen Aufträge in jedem Fall eine solche Herausgebersignatur erzeugen.

Details zum Aufbau der im Folgenden beschriebenen Geschäftsvorfälle finden sich in [Syntax].

Die Geschäftsvorfälle zum PIN/TAN-Management sollten vom Kundenprodukt immer in einem geschlossenen Kommunikationskontext, d. h. in separaten Nachrichten in einer separaten Kommunikation geschickt werden, da ansonsten eine gezielte Verarbeitung nicht gewährleistet werden kann und somit ein exaktes Wissen, ab wann z. B. eine PIN-Änderung gültig ist, nicht besteht.

Ob Aufträge zum PIN/TAN-Management isoliert gesendet werden, wird auf Kreditinstitutsseite jedoch nicht geprüft.

Grundsätzlich werden alle vom Benutzer übermittelten TANs, wenn möglich, aus Sicherheitsgründen entwertet („verbrannt").

Damit der Benutzer Informationen darüber erhält, dass eine von ihm verwendete TAN aufgrund des Abbruchs der Verarbeitung eines Geschäftsvorfalles nicht verbraucht wurde, ist vom Kreditinstitut eine entsprechende Rückmeldung zu diesem Geschäftsvorfall zu erzeugen. Ist diese Rückmeldung eingestellt worden, kann vom Benutzer die gleiche TAN noch einmal verwendet werden.

Wird vom Kreditinstitut nicht gemeldet, dass die übermittelte TAN weiterhin gültig ist, muss die Benutzerseite davon ausgehen, dass die TAN verbraucht wurde. Dies gilt auch dann, wenn der zugehörige Geschäftsvorfall aufgrund von Fehlern nicht ausgeführt wurde.

## II.6.1 Verwalten von PIN und TAN-Listen

### II.6.1.1 PIN-Änderung

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional

**a) Benutzerauftrag**

Dieser Geschäftsvorfall bewirkt das Ändern der PIN. Zum Ändern der PIN ist im Segment PIN/TAN-Signatur die alte PIN und optional eine TAN erforderlich; der Geschäftsvorfall selbst enthält die neue PIN.

Folgende Ereignisse können Auslöser zum Ändern der PIN sein:

- Erstzugang zum Online-Banking – hier ist die vom Kreditinstitut vergebene PIN durch eine persönliche PIN zu ersetzen.

  Dazu wird bei der Initialisierung vom Kreditinstitut der Code 3916 („PIN muss wegen erstmaliger Anmeldung zwangsweise geändert werden“) zurück gemeldet. Der Benutzer muss als ersten Auftrag zwingend eine PIN-Änderung senden.

- Auf Wunsch des Benutzers
- Zwangsänderung bei Verdacht auf Kompromittierung

**b) Kreditinstitutsrückmeldung**

♦ **Erläuterungen**

Es werden keine Datensegmente zurückgemeldet.

♦ **Ausgewählte Beispiele für Rückmeldungscodes**

| Code | Beispiel für Rückmeldungstext |
|---|---|
| 0020 | PIN geändert |
| 9942 | neue PIN ungültig |

**c) Bankparameterdaten**

Geschäftsvorfallspezifische Parameter existieren nicht.

### II.6.1.2 TAN-Liste anfordern

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional

**a) Benutzerauftrag**

Abhängig vom Verfahren des Kreditinstitutes muss/kann der Benutzer eine neue TAN-Liste anfordern oder diese wird automatisch erstellt.

Sofern in den BPD hinterlegt, kann der Benutzer im Auftrag eine gewünschte Anzahl an TANs angeben. Sind in den BPD hierzu keine Angaben gemacht worden, ist die gewünschte Anzahl an TANs leer zu lassen.

**b) Kreditinstitutsrückmeldung**

- **Erläuterungen**

  Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

| Code | Beispiel für Rückmeldungstext |
|---|---|
| 0010 | Auftrag entgegengenommen |

**c) Bankparameterdaten**

Die DEG „Parameter TAN-Liste anfordern“ enthält die geschäftsvorfallspezifischen Angaben.

#### II.6.1.3 TAN-Liste freischalten

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional

**a) Benutzerauftrag**

Dieser Geschäftsvorfall bewirkt das Freischalten einer TAN-Liste.

Zum Aktivieren der neuen TAN-Liste gibt es verschiedene Verfahren, die in den BPD beschrieben werden. So kann je nach BPD die Angabe einer Transaktionsnummer der alten Liste und einer Transaktionsnummer der neuen Liste ggf. inklusive einer TAN-Listennummer erforderlich sein. Die TAN der alten Liste wird in das Segment PIN/TAN-Signatur eingestellt. Die TAN der neuen Liste und die TAN-Listennummer werden, falls in den BPD verlangt, in das Auftragssegment eingestellt.

Ob bei der Freischaltung einer neuen TAN-Liste die evtl. verbleibenden TANs einer vorher aktiven Liste ungültig werden oder noch aufgebraucht werden können, geht aus der Verfahrensanleitung des jeweiligen Kreditinstituts hervor.

**b) Kreditinstitutsrückmeldung**

- **Erläuterungen**

  Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

| Code | Beispiel für Rückmeldungstext |
|---|---|
| 0020 | TAN-Liste Nr. xxx aktiviert |
| 3915 | Alte TAN-Liste ist infolge der Aktivierung einer neuen TAN-Liste ungültig |

**c) Bankparameterdaten**

Die DEG „Parameter TAN-Liste freischalten“ enthält die geschäftsvorfallspezifischen Angaben.

### II.6.2 Sperren von PIN bzw. TAN-Listen

Es ist zu unterscheiden zwischen Sperren, die vom Kreditinstitut automatisch durch eine mehrfach falsche Benutzereingabe veranlasst werden, und Sperren, die bewusst vom Benutzer initiiert werden.

#### II.6.2.1 Sperre bei mehrmaliger Falscheingabe

Bei jedem Erhalt einer falsch signierten Nachricht für einen noch nicht gesperrten Benutzer (z. B. falsche PIN oder ungültige TAN) wird der jeweilige Fehlbedienungszähler (PIN oder TAN) erhöht. Nach Überschreiten des vom Kreditinstitut vorgegebenen Wertes wird eine Sperre vorgenommen. Eine erfolgte Sperre wird dem Benutzer mittels eines Rückmeldungscodes mitgeteilt.

Sofern das Kreditinstitut dies zulässt, ist eine Entsperrung mit Hilfe des Geschäftsvorfalls „PIN-Sperre aufheben“ (siehe *II.6.2.3 PIN-Sperre aufheben*) möglich. Die Sperre hat in diesem Fall vorläufigen Charakter. Es wird der Rückmeldungscode 3931 verwendet, damit ein Kundenprodukt für das Versenden der Entsperrung den Dialog weiterhin offen halten kann.

Falls die Sperre hingegen nur vom Kreditinstitut aufgehoben werden kann (endgültige Sperre), wird der Rückmeldungscode 9931 verwendet

Der Umfang der Sperre ist kreditinstitutsabhängig und kann dem Benutzer im Rahmen der Rückmeldung detaillierter mitgeteilt werden.

- **Ausgewählte Beispiele für Rückmeldungscodes**

| Code | Beispiel für Rückmeldungstext |
|---|---|
| 3931 | Vorläufige Sperre liegt vor. Entsperren mit GV „PIN-Sperre aufheben“ möglich |
| 9931 | Online-Zugang gesperrt, Entsperren nur durch Kreditinstitut |
| 9931 | SB-Zugang gesperrt, Entsperren nur durch Kreditinstitut |
| 9931 | Konto gesperrt, Entsperren nur durch Kreditinstitut |
| 9931 | PIN gesperrt, Entsperren nur durch Kreditinstitut |

### II.6.2.2 PIN-Sperre

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional

**a) Benutzerauftrag**

Dieser Geschäftsvorfall bewirkt eine Sperre durch den Benutzer. Der Umfang der Sperre ist kreditinstitutsabhängig und kann dem Benutzer im Rahmen der Rückmeldung detaillierter mitgeteilt werden.

Das Sperren des Online-Banking-Zugangs durch den Benutzer erfordert analog zu den HBCI-Signaturverfahren DDV und RDH die Eingabe einer gültigen PIN, selbst wenn diese kompromittiert sein sollte. Diese wird im Segment PIN/TAN-Signatur eingestellt.

Der Geschäftsvorfall selbst enthält keine weiteren Daten.

**b) Kreditinstitutsrückmeldung**

- **Erläuterungen**

  Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

| Code | Beispiel für Rückmeldungstext |
|---|---|
| 0020 | PIN-Sperre erfolgreich |
| 0020 | Konto-Sperre erfolgreich |
| 0020 | Sperre erfolgreich. Zur Entsperrung wenden Sie sich bitte an Ihr Kreditinstitut |

**c) Bankparameterdaten**

Geschäftsvorfallspezifische Parameter existieren nicht.

### II.6.2.3 PIN-Sperre aufheben

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional

**a) Benutzerauftrag**

Dieses Segment bewirkt das Aufheben einer PIN-Sperre. Wurde eine Online-Sperre auf ein Konto gelegt (i. d. R. durch mehrmalige Eingabe einer falschen PIN), kann das Konto durch die Eingabe der richtigen PIN und einer gültigen TAN wieder entsperrt werden (PIN und TAN befinden sich im Segment PIN/TAN-Signatur).

Der Geschäftsvorfall selbst enthält keine weiteren Daten.

Da bei gesperrter PIN im Regelfall keine weitere Kommunikation möglich ist, kann dieser Geschäftsvorfall nur angeboten werden, wenn das Kreditinstitut nach einer PIN-Sperre weitere Kommunikationen mit der gesperrten PIN zulässt, sofern in diesen nur der Geschäftsvorfall „PIN-Sperre aufheben“ gesendet wird. Siehe dazu auch *II.6.2.1 Sperre bei mehrmaliger Falscheingabe*.

In der Regel wird kreditinstitutsseitig nur ein einziger Versuch zur Aufhebung der PIN-Sperre zugelassen. Schlägt dieser fehl, kann nur das Kreditinstitut entsperren.

**b) Kreditinstitutsrückmeldung**

- **Erläuterungen**

  Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

| Code | Beispiel für Rückmeldungstext |
|---|---|
| 0020 | PIN-Sperre aufgehoben |

**c) Bankparameterdaten**

Geschäftsvorfallspezifische Parameter existieren nicht.

#### II.6.2.4 TAN-Liste sperren/löschen

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional

**a) Benutzerauftrag**

Dieser Geschäftsvorfall bewirkt das Löschen der TAN-Liste. Diese Sperre kann je nach Kreditinstitut entweder vom Mitarbeiter wieder rückgängig gemacht werden oder führt zur automatischen Zusendung einer neuen TAN-Liste.

Je nach Parameterangaben in den BPD ist im Geschäftsvorfall eine TAN-Listennummer anzugeben oder nicht. Wird eine solche TAN-Listennummer angegeben, dann bezieht sich die Sperre allein auf die zugehörige TAN-Liste. Fehlt die Nummer, werden immer alle im Umlauf befindlichen TAN-Listen des Benutzers gesperrt.

**b) Kreditinstitutsrückmeldung**

- **Erläuterungen**

  Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

| Code | Beispiel für Rückmeldungstext |
|---|---|
| 0020 | TAN-Liste gesperrt |
| 3912 | Neue TAN-Liste wird automatisch verschickt |

**c) Bankparameterdaten**

Die DEG „Parameter TAN-Liste sperren“ enthält die geschäftsvorfallspezifischen Angaben.

### II.6.3 Sonstige

#### II.6.3.1 TAN-Verbrauchsinformationen anzeigen

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional

**a) Benutzerauftrag**

Dieses Segment bewirkt die Anzeige der verbrauchten TANs des Benutzers.

Der Geschäftsvorfall selbst enthält keine weiteren Daten.

**b) Kreditinstitutsrückmeldung**

- **Beschreibung**

  Das Response-Segment enthält je zurückzumeldender TAN-Liste eine DEG mit den zugehörigen Informationen. Diese umfassen mindestens den TAN-Listenstatus und die TAN-Listennummer. Jeweils optional können darüber hinaus das Erstellungsdatum, die Anzahl der TANs der Liste, die Anzahl der verbrauchten TANs der Liste und nähere Informationen zu den TANs selbst enthalten sein.

- **Ausgewählte Beispiele für Rückmeldungscodes**

| Code | Beispiel für Rückmeldungstext |
|---|---|
| 0020 | Auftrag ausgeführt |

**c) Bankparameterdaten**

Geschäftsvorfallspezifische Parameter existieren nicht.

### II.6.3.2 TAN prüfen und „verbrennen“

Um eine TAN prüfen und verbrennen zu lassen, wird dem Benutzer kein spezieller Geschäftsvorfall bereitgestellt. Vielmehr hat er die Möglichkeit, in einer Initialisierungsnachricht ohne Auftragsteil neben der PIN zusätzlich auch eine TAN mitzuschicken. Diese wird dann an das Kreditinstitut übermittelt und kann dann von dieser geprüft und entwertet werden. Die Ergebnisse der Prüfung und des Verbrennens werden vom Kreditinstitut als zusätzliche Returncodes innerhalb der Initialisierungsantwort zurückgemeldet.

- **mögliche Rückmeldungscodes**

| Code | Beispiel für Rückmeldungstext |
| --- | --- |
| 0900 | TAN gültig |
| 9941 | TAN ungültig |
| 3913 | TAN wurde verbraucht |

### II.6.3.3 PIN prüfen

Um eine PIN prüfen zu lassen, wird dem Benutzer kein spezieller Geschäftsvorfall bereitgestellt. Vielmehr ist diese PIN-Prüfung innerhalb der Initialisierung implizit vom Kreditinstitut durchzuführen. Der Benutzer hat somit analog zu *II.6.3.2 TAN prüfen und „verbrennen“* die Möglichkeit, eine Initialisierungsnachricht ohne Auftragsteil zu senden. Die PIN wird dann an das Kreditinstitut übermittelt und kann dort geprüft werden. Die Ergebnisse der Prüfung werden vom Kreditinstitut als zusätzliche Returncodes innerhalb der Initialisierungsantwort zurückgemeldet.

- **mögliche Rückmeldungscodes**

| Code | Beispiel für Rückmeldungstext |
| --- | --- |
| 0901 | PIN gültig |
| 9942 | PIN ungültig |