HBCI

Homebanking-Computer-Interface

- Schnittstellenspezifikation -

Erweiterung PIN/TAN

Herausgeber:
SIZ – Informatikzentrum der Sparkassenorganisation GmbH, Bonn
GAD – Gesellschaft für automatisierte Datenverarbeitung eG, Münster

Version: 1.01
Stand: 08.05.2002
Bezug: HBCI Version 2.2

Versionsführung

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

Name	Organisation	Datum	Version	Dokument	Anmerkungen
Böttcher	PPI	17.04.2002	1.0	hbci22aS10.doc	von SIZ und GAD verabschiedete Version
Stein	SIZ	24.04.2002	1.0 ZKA	hbci22_PINTAN_v10.doc	Erste Version für ZKA
Stein	SIZ	08.05.2002	1.01	hbci22_PINTAN_v1.01.doc	Kommunikationsverfahren 3 für https eingefügt Klarstellung eingefügt, dass die PIN in jeder Nachricht mitgeschickt werden muss Erläuterungen zu den GV zum PIN/TAN-Management eingefügt

Vorbemerkungen

In dieser Spezifikation wird die Erweiterung der HBCI-Spezifikation um die Verwendung von PIN und TAN als Sicherheitsverfahren beschrieben.

Die deutsche Kreditwirtschaft forciert seit Jahren das Onlinebanking mit HBCI (Homebanking Computer Interface). Mittlerweile bietet die überwiegende Zahl der Institute ihren Kunden dieses Verfahren an. HBCI konkurriert damit mit einigen anderen Verfahren, die in der Regel PIN und TAN für die Authentisierung und Autorisierung des Kunden 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 Erweiterung des HBCI-Systems um die PIN/TAN-Verfahren bietet somit die Möglichkeit, sämtliche Onlinebanking-Verfahren über eine einheitliche Plattform abzuwickeln (s. Abb. 1 und 2).

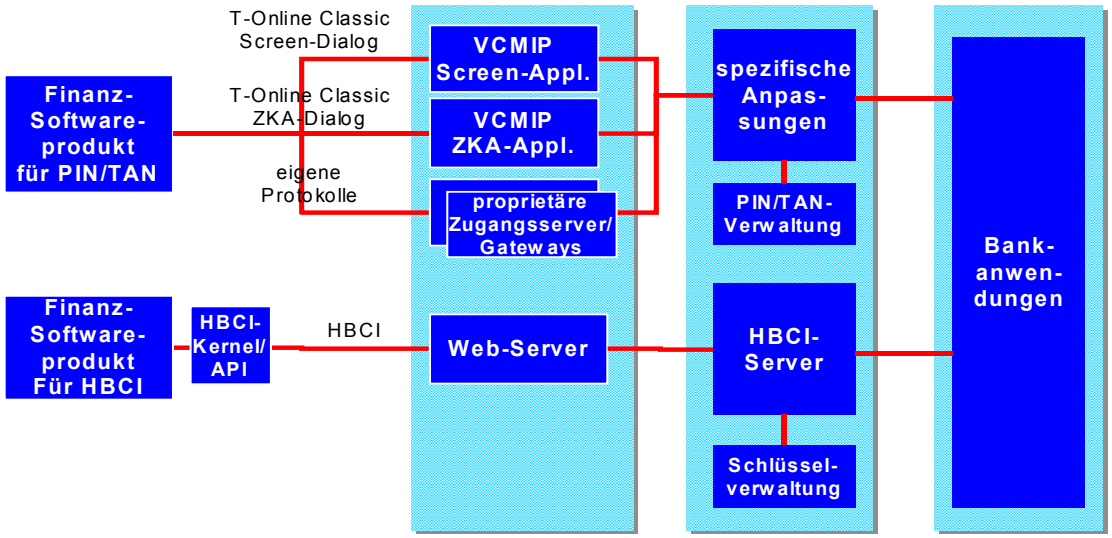

Abb. 1: Online-Banking mit PIN/TAN und HBCI traditionell

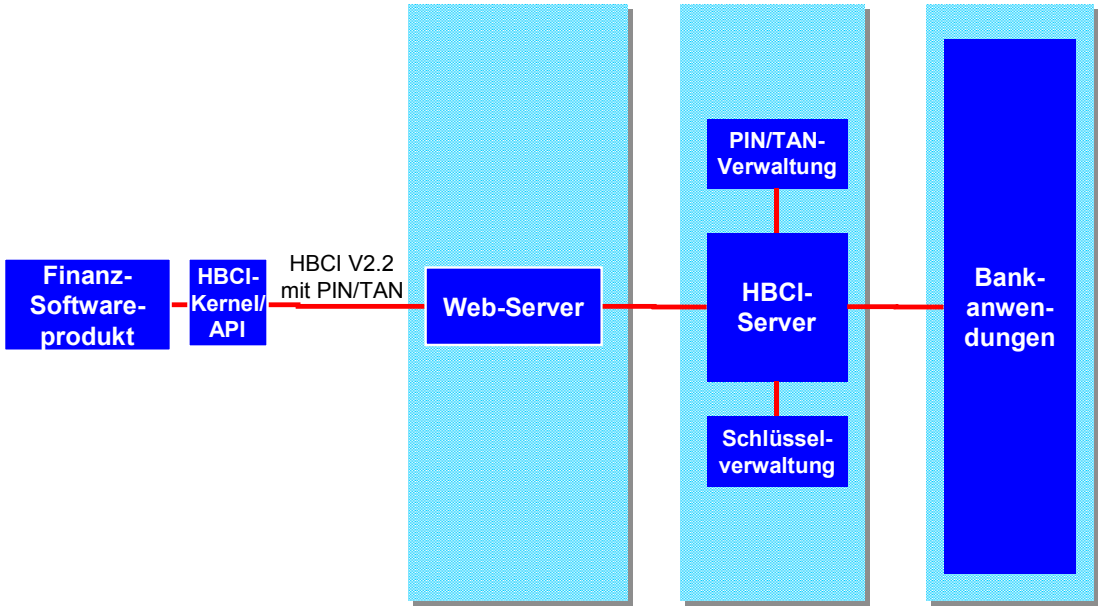

Abb. 2: Online-Banking mit HBCI PIN/TAN

Während HBCI 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 Kunde kann Onlinebanking ohne zusätzliche Infrastruktur oder Vorinstallationen betreiben. PIN/TAN ist somit eine gute Lösung für die eilige Überweisung aus dem Büro, während HBCI für die umfassende Kontenverwaltung mit einem Offline-Kundenprodukt in Frage kommt.

Die Kreditinstitute unterstützen daher oft beide Verfahren parallel. Dies führt dazu, dass der Kunde zwar aus mehreren Alternativen das für ihn bestgeeignete Verfahren auswählen kann, für die Institute 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.

Um eine möglichst einfache Integration in bestehende HBCI-System zu erlauben, wird die bestehende HBCI-Spezifikation Version 2.2 für die Integration von PIN/TAN so wenig wie möglich geändert. Somit bleiben die für den Transport der Sicherheitsinformationen definierten Segmente unverändert. Es wird lediglich eine neue DEG für

die Aufnahme von PIN und TAN definiert, die anstatt der elektronischen Signatur in den Signaturabschluss eingestellt wird. Die nicht verwendeten Datenelemente der Sicherheitssegmente werden falls notwendig mit Defaultwerten belegt. Die mit Einführung der PIN/TAN-Erweiterung verbundenen Änderungen im Kapitel VI „Sicherheit“ sind grün markiert.

Ob ein HBCI-fähiges Kreditinstitut das PIN/TAN-Verfahren anbietet, erkennt das Kundenprodukt am Vorhandensein eines HIKOM-Segmentes mit dem Kommunikationsdienst 3 (https) (s. Kap. VI.7) in den Bankparameterdaten.

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

Die Lösung verfolgt als primären Zweck das Homebanking mit Offline-Finanzsoftwareprodukten. Für HTML-Browserbanking ist der zusätzliche Einsatz eines HTML-Brokers erforderlich (s. Abb. 3).

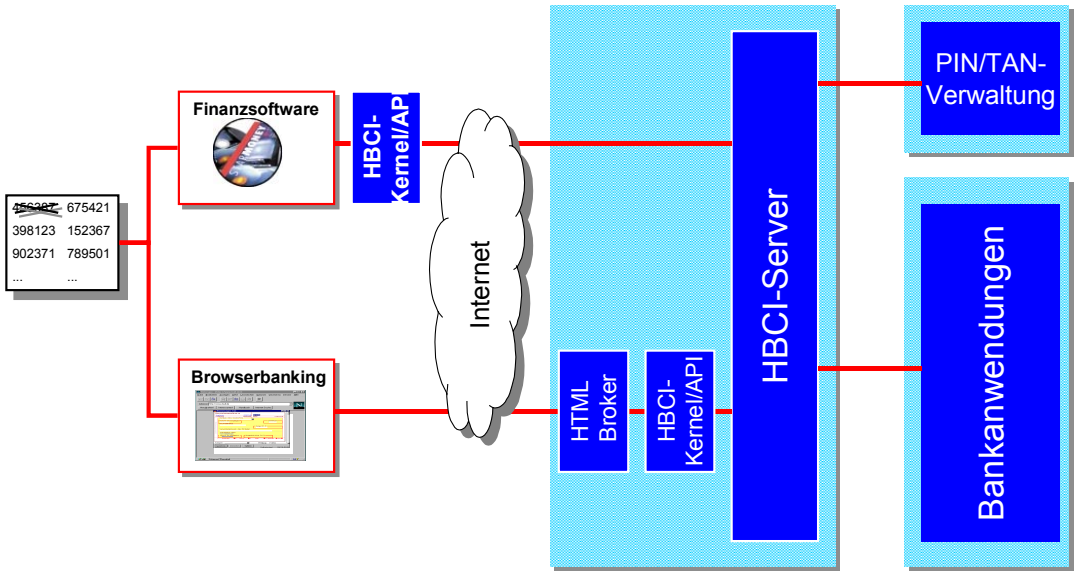

Abb. 3: Verschiedene Anwendungen für HBCI PIN/TAN

Es wird eine möglichst breite Unterstützung dieser Spezifikation auf seiten der Kundenprodukte und Kreditinstitute angestrebt, damit nach dem absehbaren Wegfall des ZKA-Dialogs weiterhin eine multibankfähige Schnittstelle für das PIN/TAN-Verfahren zur Verfügung steht.

Die Vorteile von HBCI PIN/TAN:

- Migration aller Onlinebanking-Verfahren auf Internet-Kommunikation und somit Möglichkeit zum Verzicht auf T-Online

- Im Vergleich zu T-Online/CEPT kostengünstige Homebankinglösung, da keine Datex-P-Gebühren anfallen
- Abwicklung aller Onlinebanking-Verfahren (PIN/TAN und HBCI) über eine einheitliche Plattform
- Ersatz proprietärer, inkompatibler Herstellerlösungen durch eine standardisierte Lösung aus einer Hand
- Auch für Nicht-T-Online-Kunden nutzbar
- Verfügbarkeit aller HBCI-Geschäftsvorfälle auch für PIN/TAN-Kunden
- Einheitliche Stammdatenhaltung für alle Onlinebanking-Verfahren
- Einheitliche Anbindung der Backend-Anwendungen über die HBCI'-Schnittstelle
- Kundenauthentisierung und –autorisierung an einer zentralen Stelle
- Erstmalige Standardisierung der Geschäftsvorfälle für das PIN/TAN-Management

Im folgenden gilt die Definition:

♦ **PIN/TAN-Default**

Als PIN/TAN-Default-Wert wird eine Belegung des entsprechenden Datenelementes betrachtet, welche den getroffenen Festlegungen nicht widerspricht. Ein PIN/TAN-Default ist somit ein gültiger Wert im Sinne der Definition des Datenelementes. Trotzdem ist dieser PIN/TAN-Default des betroffenen Datenelements für die Verarbeitung nicht relevant und wird daher von den verarbeitenden Systemen auf Kreditinstitutsseite ignoriert.

Handelt es sich Datenelemente mit Status „K", sollten diese leer gelassen werden. Auch hier gilt, dass Vorhandensein und Inhalt kreditinstitutsseitig nicht geprüft werden.

VI. SICHERHEIT

VI.1 Allgemeines

Im Rahmen von HBCI werden zeitgemäße Sicherheitsmechanismen und -methoden eingesetzt, welche den Missbrauch der im Bereich des Homebankings eingesetzten Systeme verhindern. Zusätzlich wird die Möglichkeit angeboten, auch das PIN/TAN-Verfahren als alternatives Verfahren zu verwenden.

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

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

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

- eine auf dem symmetrischen DES-Verfahren basierende Chipkartenlösung
- eine auf dem asymmetrischen RSA-Verfahren basierende Lösung
- das PIN/TAN-Verfahren als alternatives Verfahren

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

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

♦ **RDH-Verfahren**

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

♦ **DDV-Verfahren**

Realisierung Bank: optional (empfohlen)
Realisierung Kunde: optional

♦ **PIN/TAN-Verfahren**

Realisierung Bank: optional
Realisierung Kunde: optional

VI.2 Mechanismen

VI.2.1 Elektronische Signatur

Die Bildung der elektronischen Signatur erfolgt durch die Vorgänge

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

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

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

1. Hashing der Nachricht

Als Hash-Funktion wird der RIPEMD-160 eingesetzt. Als Initialisierungsvektor dient die binäre Zeichenfolge X'01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10 F0 E1 D2 C3'[1]. Der erzeugte Hashwert hat eine Länge von 20 Byte (=160 bit). (Das Padding der Nachricht auf die entsprechende Blockgröße ist im Hashverfahren implizit enthalten).

2. Formatierung des Hashwerts

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

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

3. Berechnung der elektronischen Signatur

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

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

1. Hashing der Nachricht

siehe „Elektronische Signatur bei DDV"

---

[1] Little-Endian-Notation

2. Formatierung des Hashwerts

Die Formatierung erfolgt gemäß ISO 9796:1991 (Kap. 5.1-5.4). Der Hashwert wird für die nachfolgende Signaturbildung als Langzahl[2] interpretiert (s. auch die Beispiele in der Anlage zu ISO 9796:1991).

3. Berechnung der elektronischen Signatur

Der Hash-Wert wird mittels RSA gemäß ISO 9796:1991 signiert. Hierbei sind auch die in den Anhängen A.4 „Signature function“ und A.5 „Verification function“ beschriebenen Operationen durchzuführen und die Anhänge B und C zu berücksichtigen.

VI.2.2 Verschlüsselung

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

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

Die ersten zwei Schritte sind für beide Verfahren identisch:

1. Der Sender erzeugt eine Zufallszahl als Nachrichtenschlüssel und stellt ungerade Parität sicher. Bei der Auswahl der Zufallszahl ist darauf zu achten, dass keiner der folgenden schwachen oder halbschwachen Schlüssel[3] gewählt wird (vgl. Kapitel VI.3.1.1).

   Die schwachen Schlüssel des DES-Algorithmus:

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

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

[3] Die schwachen und halbschwachen Schlüssel entsprechen denen des DFÜ-Abkommens.

Die halbschwachen Schlüssel des DES-Algorithmus:

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

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

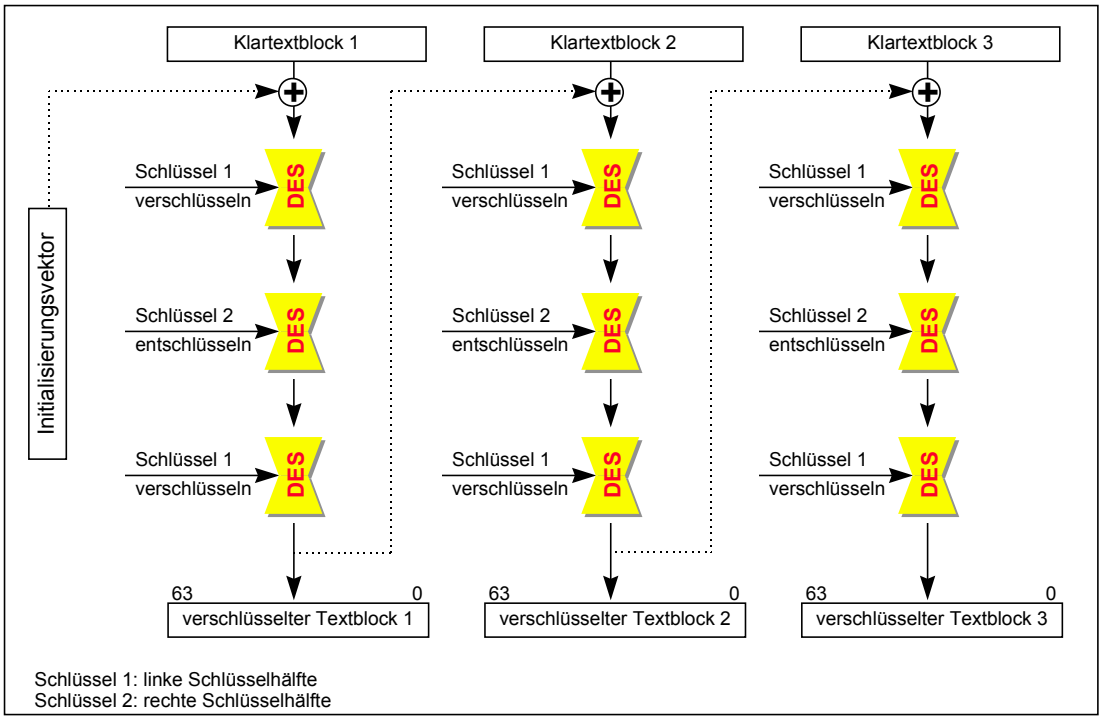

Abb. 13: 2-Key-Triple-DES im CBC-Mode

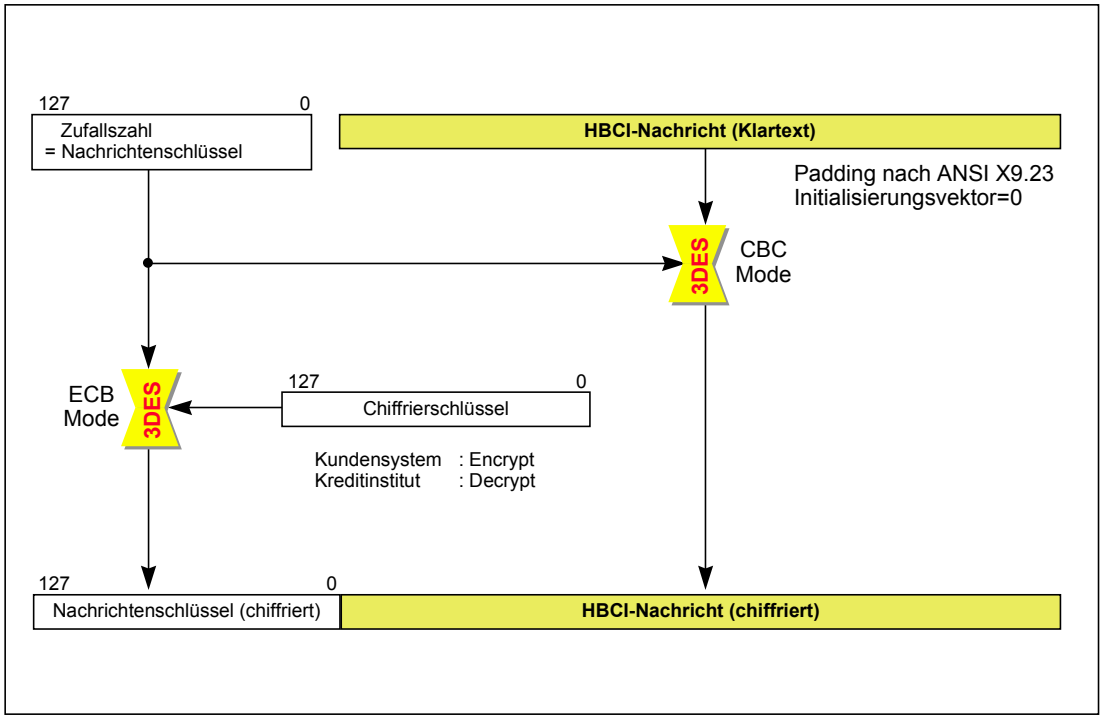

Abb. 14: Verschlüsselung bei 2-Key-Triple-DES

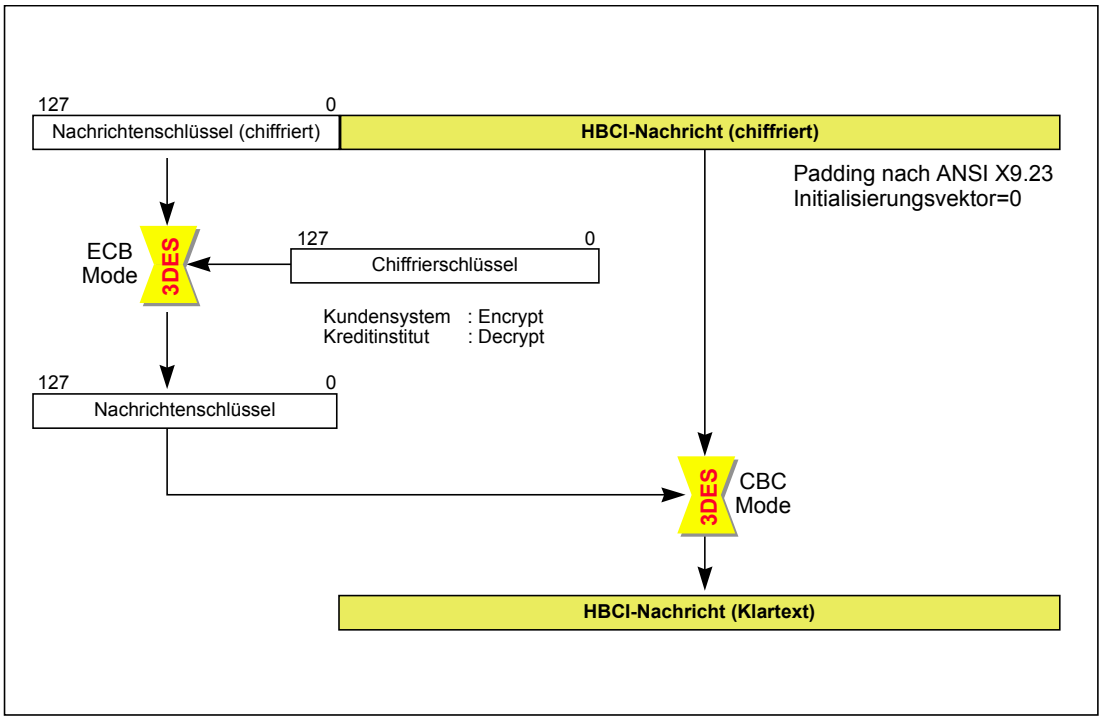

Abb. 15: Entschlüsselung bei 2-Key-Triple-DES

Die weitere Verarbeitung ist bei DDV und RDH unterschiedlich:

VI.2.2.1 Verschlüsselung bei DDV (DES-basierend)

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

   Aufgrund vorgegebener Verfahren bei der ZKA-Chipkarte wird zum Chiffrieren und Dechiffrieren des Nachrichtenschlüssels, unabhängig von der Übertragungsrichtung, kundensystemseitig immer die Routine „Encrypt“ benutzt, kreditinstitutsseitig immer die Routine „Decrypt“ (vgl. Kapitel VIII.8.5.2).

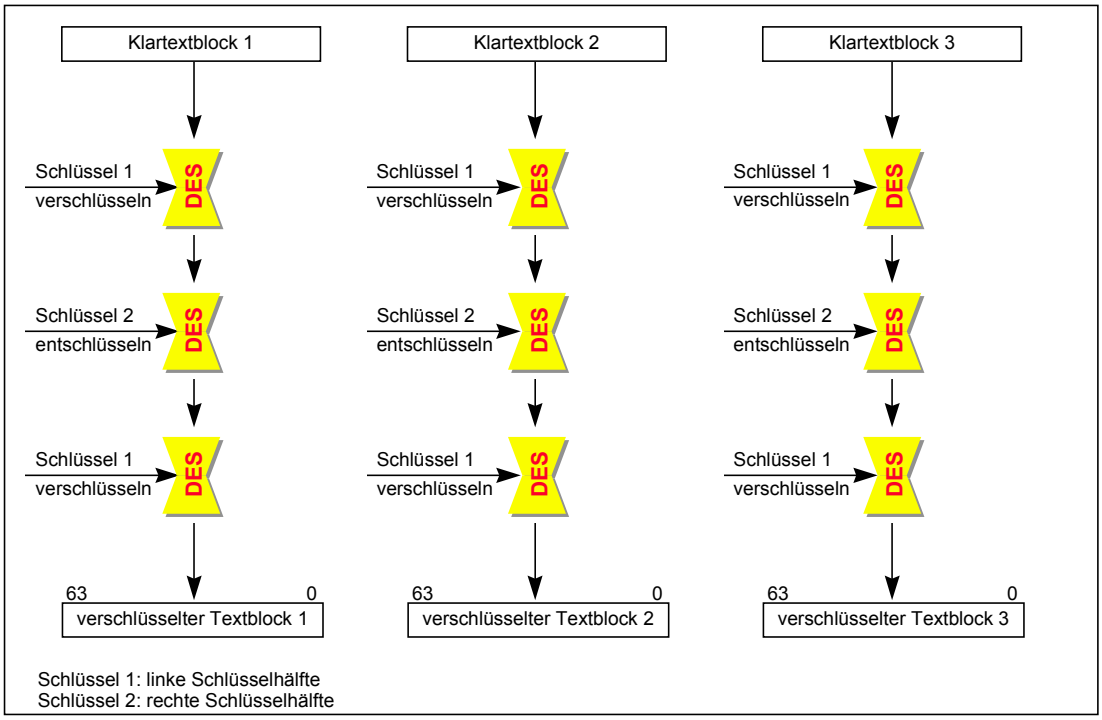

Abb. 16: 2-Key-Triple-DES im ECB-Mode

VI.2.2.2 Verschlüsselung bei RDH (RSA-basierend)

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

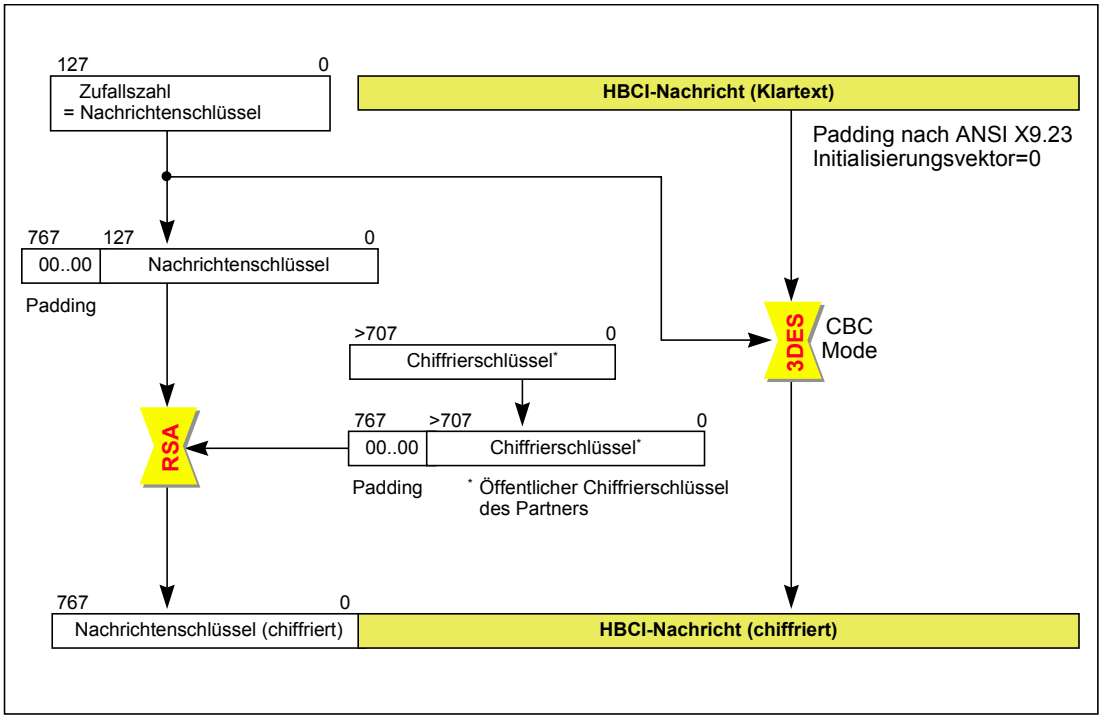

Abb. 17: Verschlüsselung bei RSA (2-Key-Triple-DES)

VI.2.3 Sicherheitsmedien beim Kundenprodukt

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

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

Es ist zwingend erforderlich, die Daten auf dem Sicherheitsmedium (kryptographisch) zu schützen. Speziell ist im Rahmen der Speicherung der Schlüsselpaare auf Diskette bzw. Festplatte sicherzustellen, dass die Daten unter Einbeziehung eines Passwortes (Banking-PIN o.ä.) verschlüsselt werden und der Zugriff auf die verschlüsselten Daten nur über die manuelle Eingabe des entsprechenden Passwortes möglich ist.

Gleiches gilt bei der Verwendung des PIN/TAN-Verfahrens.

VI.3 Abläufe

VI.3.1 Schlüsselverwaltung

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

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

VI.3.1.1 Gemeinsam verwendete Verfahren zur Schlüsselverwaltung

- **Schlüsselarten**

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

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

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

- **Schlüsselnamen**

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

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

  Falls kein öffentlicher Schlüssel des Kreditinstituts vorliegt, so ist als Versionsnummer der Wert „999“ einzustellen. Damit wird kreditinstitutsseitig auf den aktuell gültigen Schlüssel referenziert (Ein Kreditinstitut kann während einer Übergangszeit evtl. mehrere Schlüssel bis zu einem Verfallsdatum vorhalten. Aktuell gültig ist jeweils der neueste Schlüssel).

- **Generierung von Nachrichtenschlüsseln**

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

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

VI.3.1.2 Symmetrische Schlüssel für DDV

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

VI.3.1.2.1 Schlüsselgenerierung

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

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

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

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

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

♦ **Herleitung von Kartenschlüsseln:**

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

Ein kartenindividueller Schlüssel KK von 16 Byte Länge wird aus

- KGK (Key Generating Key, 16 Byte)
- CID (vollständiger Inhalt von EF_ID, mit X’00’ auf das nächste Vielfache von 8 Byte Länge aufgefüllt) und
- dem öffentlich bekannten Initialwert I = X’52 52 52 52 52 52 52 52 25 25 25 25 25 25 25 25’ (16 Byte)

zu

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

berechnet.

Hierbei bezeichnen

- ‘P’ die Funktion "Parity Adjustment" auf ungerade Parität, die wie folgt definiert ist:
  Sei $b_1,..,b_8$ die Darstellung eines Byte als Folge von 8 bit. Dann setzt P das niedrigstwertige bit b_8 jedes Byte auf ungerade Parität, d.h. b_8 wird in jedem Byte so gesetzt, dass es eine ungerade Anzahl von 1 enthält.

- ‘d * KGK’ die 2-Key-Triple-DES-Entschlüsselung im ECB-Mode (ISO 10116) mit dem Schlüssel KGK.
- ‘H’ die in ISO 10118-2 definierte Hash-Funktion.

VI.3.1.2.2 Initiale Schlüsselverteilung

Die initiale Schlüsselverteilung erfolgt implizit mit der Verteilung der Chipkarte.

VI.3.1.2.3 Schlüsseländerungen

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

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

VI.3.1.2.4 Schlüsselverteilung nach Kompromittierung

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

VI.3.1.3 Asymmetrische Schlüssel für RDH

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

- ein Signierschlüsselpaar
- ein Chiffrierschlüsselpaar

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

Falls ein Kreditinstitut seine Nachrichten nicht signiert, kann es auf das Signier-Schlüsselpaar verzichten.

VI.3.1.3.1 Schlüsselgenerierung

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

Die Schlüsselgenerierung hat gemäß dem folgenden Ablauf stattzufinden:[4]

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

    Die entsprechenden Forderungen werden an q gestellt.

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

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

---

[4] Das Verfahren entspricht dem des DFÜ-Abkommens.

[5] Der Primteiler sollte dabei ungefähr der Länge des Schlüssels entsprechen.

VI.3.1.3.2 Initiale Schlüsselverteilung

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

- seine Benutzerkennung
- Informationen zum Kommunikationszugang

Die Übermittlung dieser Informationen ist auf zwei Wegen denkbar:

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

Zu Beginn muss ein gegenseitiger Austausch der öffentlichen Schlüssel von Kunde und Kreditinstitut erfolgen.[6]

Hierzu ist folgender Ablauf vorgesehen:

1. Das Kreditinstitut übermittelt seinen öffentlichen Chiffrierschlüssel an den Kunden. Falls es Nachrichten signiert, übermittelt es ebenfalls seinen öffentlichen Signierschlüssel. Hierzu gibt es zwei Möglichkeiten:
   - Zusenden bzw. Aushändigung der Schlüssel und anderer relevanter Daten auf einem Medium (z.B. Diskette[7], Chipkarte) bei Vertragseröffnung.

   Falls dem Kunden eine Diskette zugesendet wird, hat diese folgende Daten zu enthalten:
   - Datei mit ein bzw. zwei Segmenten vom Typ HIISA, die jeweils einen öffentlichen Schlüssel des Kreditinstitutes enthalten
   - BPD des Kreditinstitutes
   - Übertragung der Schlüssel beim Erstzugang

     (1) Der Kunde fordert beide öffentlichen Schlüssel und die BPD mit Hilfe der Key-Management-Nachricht „Erstmalige Anforderung der Schlüssel des Kreditinstituts“ (s. Kap. VI.6.2.2) an. Diese Nachricht ist weder signiert noch chiffriert.

     (2) Der weitere Ablauf ist abhängig davon, ob das Kreditinstitut seine Antwortnachrichten signiert.

---

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

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

Fall A: Das Kreditinstitut signiert

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

Fall B: Das Kreditinstitut signiert nicht

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

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

a) Padding der höchstwertigen Bits von Exponent und Modulus des Schlüssels mit Nullen (X'00') auf 1024 Bit

b) Konkatenierung von Exponent und Modulus (Exponent || Modulus)

c) Bildung des Hashwerts mittels RIPEMD-160 gemäß Kap. VI.2.1.1 über diesen Ausdruck

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

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

(5) Bei Übereinstimmung der Hashwerte gelten die öffentlichen Schlüssel des Kreditinstituts als authentisiert.

2. Es hat eine Synchronisierung der Signatur-ID zu erfolgen (s. Kap. III.8). Dabei ist als Kundensystem-ID der Wert ‚0' zu verwenden.

3. Der Kunde übermittelt seine beiden öffentlichen Schlüssel, die mit dem privaten Signierschlüssel unterzeichnet wurden, im Rahmen der Key-Management-Nachricht „Erstmalige Übermittlung der Schlüssel des Kunden" an das Kreditinstitut (vgl. Kapitel VI.6.2.3). Diese Nachricht muss sowohl signiert als auch chiffriert sein.

4. Begleitet wird diese Nachricht durch einen Ini-Brief gemäß dem in Abbildung 18 aufgeführten Muster. Im Ini-Brief bestätigt der Kunde ausschließlich den öffentlichen Signierschlüssel mit handschriftlicher Unterschrift. Eine Bestätigung des öffentlichen Chiffrierschlüssels ist nicht erforderlich, da dieser mit dem Signierschlüssel signiert wird und damit authentifiziert ist. Neben dem Schlüssel und dem Schlüsselnamen wird im Ini-Brief der Hashwert des Schlüssels aufgeführt. Dieser wird ebenso gebildet wie der Hashwert im Ini-Brief des Kreditinstituts (s.o.).

5. Im Kreditinstitut findet ein Vergleich zwischen dem im Ini-Brief aufgeführten Hashwert und dem Hashwert des vom Kunden übermittelten öffentlichen Signierschlüssels statt.
6. Falls dieser Vergleich positiv verläuft, werden die öffentlichen Schlüssel des Kunden freigeschaltet.
7. Es hat eine Synchronisierung der Kundensystem-ID zu erfolgen (s. Kap. III.8).
8. Nachdem die Erstinitialisierung abgeschlossen ist, kann der Kunde Auftragsnachrichten senden.

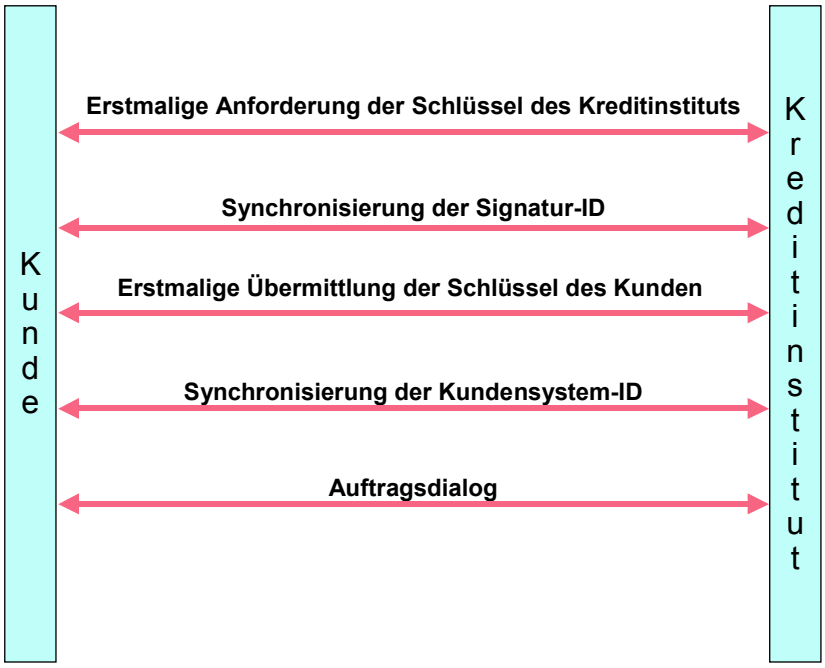

Abb. 18: Ablauf der Erstinitialisierung bei RDH

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

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

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

Ini-Brief HBCI

Benutzername	_____	Kundensoftware-interner Name (Angabe freigestellt)
Datum	_____	Datum der Erstellung des Initialisierungsauftrags (TT.MM.JJJJ)
Uhrzeit	_____	Uhrzeit der Erstellung des Initialisierungsauftrags (hh:mm)
Empfänger	_____	Kreditinstitutskennung (wird vom jeweiligen Kreditinstitut mitgeteilt)
Benutzerkennung	_____	max. 30 Stellen alphanumerisch (wird vom jeweiligen Kreditinstitut mitgeteilt)
Schlüsselnummer	_____	Nummer des Signierschlüssels (max. 3 Stellen)
Schlüsselversion	_____	Version des Signierschlüssels (max. 3 Stellen)
HBCI-Version	_____	derzeit 2.2

Öffentlicher Schlüssel für die elektronische Signatur:

Exponent 0768

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01
```

Modulus 0768

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

Hash E4 DB 82 22 1E D6 51 4B A9 8F
65 E9 F9 25 B3 0D 2A 23 EC 50

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

_____	_____	_____
Ort / Datum	Firma/Name	Unterschrift

Abb. 19: Beispiel für die Gestaltung des Ini-Briefs

VI.3.1.3.3 Schlüsseländerungen

- **Routinemäßige Schlüsseländerung des Kunden**

  Ein Kunde ändert seine Signier- und Chiffrierschlüsselpaare unabhängig.

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

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

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

- **Routinemäßige Schlüsseländerung des Kreditinstituts**

  Ein Kreditinstitut generiert bei Bedarf ein neues Schlüsselpaar.

  Der Kunde sendet jeweils bei der Dialoginitialisierung die Referenz auf die öffentlichen Schlüssel des Kreditinstitutes mit (vgl. Kapitel III.3.1). Falls das Kreditinstitut über aktuellere öffentliche Schlüssel verfügt, werden diese in der Kreditinstitutsnachricht mitübertragen (vgl. Kapitel III.3.2 respektive VI.6.1.3). Die neuen Schlüssel gelten ab sofort, d.h. bereits für die erste Auftragsnachricht nach der Dialoginitialisierung. Da das Kreditinstitut i.d.R. aber auch noch die alten Schlüssel aktiv hält, werden für einen begrenzten Zeitraum auch noch Nachrichten akzeptiert, die mit den alten Kreditinstitutsschlüsseln chiffriert wurden.

  Für den Fall, dass der alte Kreditinstitutsschlüssel nicht mehr zur Verfügung steht oder gesperrt werden musste, wird dem Kunden - falls er den alten Kreditinstitutsschlüssel bei der Dialoginitialisierung verwendet – der Rückmeldungscode "9030" mit dem Hinweis "Fehler beim Entschlüsseln" gesendet. Daraufhin sollte das Kundenprodukt die neuen Kreditinstitutsschlüssel anfordern.

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

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

VI.3.1.3.4 Schlüsselverteilung nach Kompromittierung

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

VI.3.2 Schlüsselsperrung

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

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

Zusätzlich müssen bei der Sperrung noch folgende Punkte berücksichtigt werden:

- Information des Kunden
- Entsperrung

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

♦ **Kompromittierung des eigenen Schlüssels**

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

♦ **Verlust des eigenen Schlüssels**

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

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

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

♦ **Überschreiten der Anzahl der Falschsignaturen**

Wird beim Einreichen von Aufträgen durch fehlerhafte Signaturen die festgelegte Anzahl von n Falschsignaturen in Folge überschritten, wird kreditinstitutsseitig der Schlüssel gesperrt. Als Falschsignaturen werden dabei fehlgeschlagene kryptographische Operationen, jedoch z.B. keine fehlerhaften Berechtigungen verstanden.

Bei einer Sperrung aufgrund zu vieler Fehlsignaturen werden sowohl Signier- als auch Chiffrierschlüssel gesperrt. Sofern die Nachricht lediglich von einem einzigen Benutzer signiert wurde oder falls bei einer mehrfach signierten Nachricht der Dialogführer von der Fehlsignaturensperre betroffen ist, wird der Dialog beendet. Der Dialogabbruch erfolgt dabei kreditinstitutsseitig im Anschluss an die Antwortnachricht, d.h. ein Austausch von Dialogbeendigungsnachrichten findet nicht statt. Die Antwort ist beim DDV-Verfahren weder signiert noch verschlüsselt. Beim RDH-Verfahren ist die Antwort signiert (sofern kreditinstitutsseitig signiert wird) aber nicht verschlüsselt. In der Antwortnachricht teilt das Kreditinstitut lediglich den Grund des

Dialogendes mit. Antworten auf Aufträge dürfen nicht mitgesendet werden, da diese aufgrund der Sperrung nicht abgesichert werden können.

- **Information des Kunden**

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

- **Entsperrung der Benutzerkennung**

  Eine Entsperrung erfolgt nur gegen handschriftliche Unterschrift des Kunden.

  Ist der Schlüssel kompromittiert oder nicht mehr auffindbar, so wird für den Benutzer eine neue Chipkarte, respektive neue Schlüssel und ein neues EF_ID (DDV), oder ein neues Schlüsselpaar (RDH) erzeugt und der alte Schlüssel bleibt gesperrt. Es werden in jedem Falle beide Schlüsselpaare neu vergeben, auch wenn nur ein Schlüsselpaar kompromittiert sein sollte. Damit ein Benutzer nach einer Sperrung wieder zum Zugang zum System autorisiert werden kann, darf er in diesem Fall ausnahmsweise einer erneute Erstinitialisierung durchführen und seine Schlüssel über einen Ini-Brief freischalten lassen.

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

VI.4 Bankfachliche Anforderungen

- **Zu signierende Nachrichten**

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

  Die Signatur von Kreditinstitutsnachrichten ist optional.

- **Doppeleinreichungskontrolle**

  Die Doppeleinreichungskontrolle wird für DDV und RDH mittels eines Zählers pro Signatur realisiert (Signatur-ID), dessen Inhalt jeweils in die Signatur(en) der Nachricht einfließt. Beim RDH-Verfahren wird zur Doppeleinreichungskontrolle z.Zt. zusätzlich zur Signatur-ID die Kundensystem-ID benötigt.

  Im PIN/TAN-Verfahren werden keine Signatur-IDs benötigt, da hier die TAN deren Aufgabe übernimmt und durch sie eine Doppeleinreichung verhindert wird. Eine Kundensystem-ID ist jedoch auch hier notwendig, da das zugrundeliegende Sicherheitsmedium potentiell kopierbar ist und der gleiche HBCI-Benutzer daher zeitgleich mehrere Dialoge von verschiedenen Kundensystemen aus führen kann.

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

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

- **Mehrfachsignaturen**

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

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

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

VI.5 Formate für Signatur und Verschlüsselung

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

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

HNHBK	HNSHK	HBCI-Nutzdaten	HNSHA	HNHBS

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

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

HNHBK	$HNSHK_2$	$HNSHK_1$	HBCI-Nutzdaten	$HNSHA_1$	$HNSHA_2$	HNHBS

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

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

HNHBK	HNVSK	$e_k(HNSHK_n \mid \text{HBCI-Nutzdaten} \mid HNSHA_n)$	HNHBS

Grundsätzlich erfolgt die Reihenfolge der Sicherheitsverarbeitung in folgender Reihenfolge:

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

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

VI.5.1 Mehrfach verwendete Datenelementgruppen

VI.5.1.1 Schlüsselname

- **Beschreibung**

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

- **Format**

  Name: Schlüsselname
  Typ: Datenelementgruppe

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

- **Erläuterungen**

  Nr. 1: Kreditinstitut

  In diesem „mehrfach verwendeten HBCI-Element“ werden Kreditinstitutskennung (Bankleitzahl) und Länderschlüssel abgespeichert (vgl. Kapitel II.5.3.2).

  Nr. 2: Benutzerkennung

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

  Bei Schlüsseln des Kreditinstituts ist eine beliebige Kennung einzustellen, die dazu dient, den Kreditinstitutsschlüssel eindeutig zu identifizieren. Diese Kennung darf weder einer anderen gültigen Benutzerkennung des Kreditinstituts noch der Benutzerkennung für den anonymen Zugang entsprechen.

  Nr. 3: Schlüsselart

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

  Abhängig vom Verwendungszweck kann die Schlüsselart zwei Werte annehmen:

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

  Nr. 4: Schlüsselnummer

  PIN/TAN-Default, z.B. „0“

  Nr. 5: Schlüsselversion

  PIN/TAN-Default, z.B. „0“

VI.5.1.2 Sicherheits-/Gültigkeitsdatum und -uhrzeit

♦ **Beschreibung**

Enthält einen Zeitstempel, sowie dessen Bedeutung.

♦ **Format**

Name: Sicherheitsdatum und -uhrzeit
Typ: Datenelementgruppe

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

♦ **Erläuterungen**

Nr. 1: Datum- und Zeitbezeichner, kodiert

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

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

Nr. 2: Datum

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

Nr. 3: Uhrzeit

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

VI.5.1.3 Sicherheitsidentifikation, Details

♦ **Beschreibung**

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

♦ **Format**

Name: Sicherheitsidentifikation, Details
Typ: Datenelementgruppe

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

♦ **Erläuterungen**

Die Gruppendatenelemente Nr. 2 bzw. 3 müssen alternativ gefüllt sein.

Nr. 1: Bezeichner für Sicherheitspartei

Identifikation der Funktion der beschriebenen Partei, in diesem Falle des Kunden.

Es sind folgende Werte vorgesehen:

- "1" für ‘MS’ (Message Sender), wenn ein Kunde etwas an sein Kreditinstitut sendet.
- "2" für ‘MR’ (Message Receiver), wenn das Kreditinstitut etwas an seinen Kunden sendet.

Nr. 2: CID

Dieses Feld darf für PIN/TAN nicht belegt werden.

Nr. 3: Identifizierung der Partei

Dieses Feld muss für PIN/TAN eine gültige, zuvor vom HBCI-System angeforderte Kundensystem-ID enthalten (analog zum RSA-Verfahren). Dies gilt auch für Zweit- und Drittsignaturen.

VI.5.1.4 Zertifikat

♦ **Beschreibung**

Bei einem späteren Einsatz von Zertifizierungsinstanzen werden im Rahmen von HBCI-Nachrichten auch Zertifikate transparent verschickt. Diese werden durch Zertifikatstyp und -inhalt beschrieben.

Da Zertifikate Informationen beinhalten, die auch in den HBCI-Formaten enthalten sind (z.B. Zertifikatsreferenz respektive Schlüsselnamen), können Daten redundant vorkommen. Diese müssen dann auf Konsistenz überprüft werden, bei Unstimmigkeiten hat das Zertifikat Vorrang.

♦ **Format**

Name: Zertifikat
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Zertifikatstyp	GD	num	1	M	1	1, 2, 3
2	Zertifikatsinhalt	GD	bin	.. 2048	M	1	

♦ **Erläuterungen**

Nr. 1: Zertifikatstyp

Kennzeichnet Aufbau und Inhalt des Zertifikats.

Es sind folgende Werte vorgesehen:

- "1" für ZKA
- "2" für UN/EDIFACT
- "3" für X.509

Nr. 2: Zertifikatsinhalt

Hier wird das Zertifikat selbst transparent eingestellt.

VI.5.1.5 Öffentlicher Schlüssel

♦ **Beschreibung**

Dieses Format wird nur bei RDH-Key-Management verwendet und dient zum Transport des öffentlichen Schlüssels zwischen Kunde und Kreditinstitut bzw. umgekehrt.

♦ **Format**

Name: Öffentlicher Schlüssel
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Verwendungszweck für öffentlichen Schlüssel	GD	an	..3	M	1	5, 6
2	Operationsmodus, kodiert	GD	an	..3	M	1	16
3	Verfahren Benutzer	GD	an	..3	M	1	10
4	Wert für Modulus	GD	bin	..512	M	1	
5	Bezeichner für Modulus	GD	an	..3	M	1	12
6	Wert für Exponent	GD	bin	..512	M	1	65537
7	Bezeichner für Exponent	GD	an	..3	M	1	13

♦ **Erläuterungen**

Nr. 1: Verwendungszweck für öffentlichen Schlüssel

Kennzeichnet den Verwendungszweck für den öffentlichen Schlüssel. Diese Information muss konsistent zum Datenelement „Schlüsselart“ im Segment „Schlüsselname“ (vgl. Kapitel VI.5.1.1) gehalten werden.

Es sind folgende Werte vorgesehen:

- "5" für OCF, Owner Ciphering (Chiffrierschlüssel)
- "6" für OSG, Owner Signing (Signierschlüssel)

Nr. 2: Operationsmodus, kodiert

Es ist folgender Wert vorgesehen:

- "16" für DSMR (ISO 9796)

Nr. 3: Verfahren Benutzer

Es sind folgende Werte zugelassen:

- "10" für RSA

Nr. 4: Wert für Modulus

Enthält den Modulus des öffentlichen Schlüssels.

Nr. 5: Bezeichner für Modulus

Enthält den Bezeichner für „Modulus“.

- "12" für MOD, Modulus

Nr. 6: Wert für Exponent

Der Wert für den Exponenten des öffentlichen Schlüssels ist

- "65537"

Nr. 7: Bezeichner für Exponent

Enthält den Bezeichner für „Exponent“.

- "13" für EXP, Exponent

VI.5.2 Signaturkopf

VI.5.2.1 Segmentbeschreibung

♦ **Beschreibung**

Der Signaturkopf enthält Informationen über den damit verbundenen Sicherheitsservice, sowie über den Absender.

♦ **Format**

Name: Signaturkopf
Typ: Segment
Segmentart: Administration
Kennung: HNSHK
Bezugssegment: -
Segmentversion: 3
Sender: Kunde/Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Sicherheitsfunktion, kodiert	DE	an	..3	M	1	1, 2, 999
3	Sicherheitskontrollreferenz	DE	an	..14	M	1	<>0
4	Bereich der Sicherheitsapplikation, kodiert	DE	an	..3	M	1	1
5	Rolle des Sicherheitslieferanten, kodiert	DE	an	..3	M	1	1, 3, 4
6	Sicherheitsidentifikation, Details	DEG			M	1	
7	Sicherheitsreferenznummer	DE	num	..16	M	1	
8	Sicherheitsdatum und –uhrzeit	DEG			M	1	
9	Hashalgorithmus	DEG			M	1	
10	Signaturalgorithmus	DEG			M	1	
11	Schlüsselname	DEG			M	1	
12	Zertifikat	DEG			K	1	

♦ **Erläuterungen**

Nr. 2: Sicherheitsfunktion, kodiert

Spezifiziert die auf die Nachricht angewendete Sicherheitsfunktion.

Im Zusammenhang mit elektronischen Signaturen sind folgende Werte möglich:

- „1“ für NRO, Non-Repudiation of Origin (für RDH)
- „2“ für AUT, Message Origin Authentication (für DDV)
- „999“ für PIN/TAN

Nr. 3: Sicherheitskontrollreferenz

Die Sicherheitskontrollreferenz stellt die Verbindung zwischen Signaturkopf und dazu gehörigem Signaturabschluss (s. Kap. VI.5.3) her. Sie muss mit dem entsprechenden Feld im Signaturabschluss übereinstimmen.

Nr. 4: Bereich der Sicherheitsapplikation, kodiert

Definiert, welche Daten vom kryptographischen Prozess verarbeitet werden. Wird benötigt um z.B. zwischen relevanter und belangloser Reihenfolge von Signaturen zu unterscheiden (vgl. Kapitel VI.4).

Es sind folgende Werte möglich:

- "1" für SHM (Signaturkopf und HBCI-Nutzdaten)
- "2" für SHT (von Signaturkopf bis Signaturabschluss)

Wenn SHM gewählt wird, so bedeutet dies, dass nur über den eigenen Signaturkopf sowie die HBCI-Nutzdaten ein Hashwert gebildet wird, der in die Signatur eingeht. Dies entspricht bei Mehrfachsignaturen einer bedeutungslosen Reihenfolge.

Wenn SHT gewählt wird, dann werden auch alle schon vorhandenen Signaturköpfe und -abschlüsse mitsigniert. Das heißt, dass die Reihenfolge der Signaturen relevant ist.

Der einzig zugelassene Wert ist "1", d.h. SHM.

Nr. 5: Rolle des Sicherheitslieferanten, kodiert

Beschreibt das Verhältnis desjenigen, der die Sicherheit gewährleistet, bezüglich der zu sichernden Nachricht.

Es sind folgende Werte möglich:

- "1" für ISS, Herausgeber der signierten Nachricht (z.B. Erfasser oder Erstsignatur)
- "3" für CON, der Unterzeichnete unterstützt den Inhalt der Nachricht (z.B. bei Zweitsignatur)
- "4" für WIT, der Unterzeichnete ist Zeuge (z.B. Übermittler), aber für den Inhalt der Nachricht nicht verantwortlich

Die Wahl ist von der bankfachlichen Auslegung der Signatur, respektive vom vertraglichen Zustand zwischen Kunde und Kreditinstitut abhängig.

Der Inhalt dieses Feldes sollte derzeit nicht ausgewertet werden. Optional können aber die nachfolgenden Festlegungen angewendet werden, sofern dies zwischen Kunde und Kreditinstitut zuvor vereinbart wurde:

1. **Dialoginitialisierung und -ende:**

   Die Rolle wird durch den Dialogführenden bestimmt. Es ist nur eine Signatur erlaubt. Erlaubte Kombinationen sind ISS/wert1[8] und WIT/wert1.

2. **Auftragsnachricht:**

   Grundsätzlich gilt: Sobald die Rolle „WIT“ verwendet wird, muss dieser Benutzer mit der Benutzerkennung aus der Dialoginitialisierung arbeiten.

[8] Die Notation gibt die Rolle gefolgt von der Benutzerkennung an.

Auch der Benutzer „WIT“ muss bankseitig entsprechend der Auftragsart am Konto des Benutzers „ISS“ berechtigt sein.

Die Reihenfolge der Signaturen ist beliebig.

Anzahl Signaturen	Erlaubte Kombinationen		
	1. Signatur	2. Signatur	3. Signatur
1	ISS/wert1	-	-
2	ISS/wert1	CON/beliebig	-
	WIT/wert1	ISS/beliebig	-
3	WIT/wert1	ISS/beliebig	CON/beliebig

Auch bei Belegung dieses Feldes kann das Kundenprodukt nicht davon ausgehen, dass das Feld kreditinstitutsseitig ausgewertet wird.

Nr. 6: Sicherheitsidentifikation, Details

Identifikation der im Sicherheitsprozess involvierten Parteien. Dient zur Übermittlung der CID im DDV-Verfahren bzw. der Kundensystem-ID im RDH- und PIN/TAN-Verfahren.

Details siehe VI.5.1.3

Nr. 7: Sicherheitsreferenznummer

Sicherheitsrelevante Nachrichtenidentifikation (Signatur-ID), welche zur Verhinderung der Doppeleinreichung, respektive Garantie der Nachrichtensequenzintegrität eingesetzt werden kann.

Bei chipkartenbasierten Verfahren ist der Sequenzzähler der Chipkarte (s. Kap. VIII.8.21.910 bzw. VIII.8.2.10) einzustellen. Bei softwarebasierten Verfahren wird die Sicherheitsreferenznummer auf Basis der Kundensystem-ID und des Schlüsselnamens (Benutzerkennung) verwaltet.

Nr. 8: Sicherheitsdatum und -uhrzeit

Gibt Datum und Uhrzeit des lokalen Rechners an, an dem die Unterschrift geleistet wurde. Als Bedeutung wird „1“ eingestellt, da es sich um einen Sicherheitszeitstempel handelt.

Details siehe VI.5.1.2

Nr. 9: Hashalgorithmus

Enthält einen kryptographischen Algorithmus, seinen Operationsmodus, sowie dessen Einsatz.

Details siehe VI.5.2.2

Nr. 10: Signaturalgorithmus

Enthält einen kryptographischen Algorithmus, seinen Operationsmodus, sowie dessen Einsatz.

Details siehe VI.5.2.3

Nr. 11: Schlüsselname

Enthält den verwendeten Schlüsselnamen, respektive die Referenz auf den Schlüssel.

Details siehe VI.5.1.1

Nr. 12: Zertifikat

Hier wird bei späterem Einsatz von Zertifizierungsinstanzen ein Zertifikat transparent eingestellt.

Details siehe VI.5.1.4

Diese DEG wird bei PIN/TAN nicht verwendet.

- **Beispiel**

```
HNSHK:2:3+1+654321+1+1+1::2+3234+1:19960605:1111
44+1:999:1+6:10:16+280:10020030:12345:S:1:1'
```

VI.5.2.2 Hashalgorithmus

♦ **Beschreibung**

Enthält einen kryptographischen Algorithmus, seinen Operationsmodus, so wie dessen Einsatz, in diesem Fall für RIPEMD-160 als verwendeter Hashalgorithmus.

♦ **Format**

Name: Hashalgorithmus
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Verwendung des Hashalgorithmus, kodiert	GD	an	..3	M	1	1
2	Hashalgorithmus, kodiert	GD	an	..3	M	1	999
3	Bezeichner für Hashalgorithmusparameter	GD	an	..3	M	1	1
4	Wert des Hashalgorithmusparameters	GD	bin	..512	K	1	

♦ **Erläuterungen**

Nr. 1: Verwendung des Hashalgorithmus, kodiert

Spezifiziert die Verwendung des in Feld 2 identifizierten Algorithmus.

Im Zusammenhang mit Hash-Funktionen ist derzeit nur folgender Wert möglich:

- "1" für OHA, Owner Hashing

Nr. 2: Hashalgorithmus, kodiert

Spezifiziert den verwendeten Hash-Algorithmus:

- "999" für ZZZ, gegenseitig vereinbart (RIPEMD-160).

Nr. 3: Bezeichner für Hashalgorithmusparameter

Dies bedingt den folgenden Wert:

- "1" für IVC, Initialization value, clear text

Nr. 4: Wert des Hashalgorithmusparameters

Dieses Feld muss nicht belegt werden. Wenn ja, muss es einen PIN/TAN-Defaultwert enthalten.

♦ **Beispiel**

```
1:999:1
```

VI.5.2.3 Signaturalgorithmus

♦ **Beschreibung**

Enthält einen kryptographischen Algorithmus, seinen Operationsmodus, so wie dessen Einsatz, in diesem Fall für die Signaturbildung über DDV bzw. RDH.

♦ **Format**

Name: Signaturalgorithmus
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Verwendung des Signaturalgorithmus, kodiert	GD	an	..3	M	1	6
2	Signaturalgorithmus, kodiert	GD	an	..3	M	1	1, 10
3	Operationsmodus, kodiert	GD	an	..3	M	1	16, 999

♦ **Erläuterungen**

Nr. 1: Verwendung des Signaturalgorithmus, kodiert

Spezifiziert die Verwendung des in Feld 2 identifizierten Algorithmus.

Im Zusammenhang mit Signaturbildung ist derzeit nur folgender Wert möglich:

- "6" für OSG, Owner Signing

Nr. 2: Signaturalgorithmus, kodiert

PIN/TAN-Default, z.B. „10“

Nr. 3: Operationsmodus, kodiert

PIN/TAN-Default, z.B. „16“

♦ **Beispiel**

```
6:10:16
```

VI.5.3 Signaturabschluss

- **Beschreibung**

  Der Signaturabschluss stellt die Verbindung mit dem dazugehörigen Signaturkopf her und enthält als "Validierungsresultat" die elektronische Signatur.

- **Format**

  Name: Signaturabschluss
  Typ: Segment
  Segmentart: Administration
  Kennung: HNSHA
  Bezugssegment: -
  Segmentversion: 1
  Sender: Kunde/Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Sicherheitskontrollreferenz	DE	an	..14	M	1	<>0
3	Validierungsresultat	DE	bin	..512	K	1	
4	PIN/TAN	DEG			K	1	

- **Erläuterungen**

  Nr. 2: Sicherheitskontrollreferenz

  Stellt die Verbindung zwischen Signaturkopf und -abschluss sicher. Es enthält den gleichen Wert, wie das gleichnamige Feld im Signaturkopf.

  Nr. 3: Validierungsresultat

  Dieses Feld muss nicht belegt werden. Es kann aber einen PIN/TAN-Defaultwert enthalten.

  Nr. 4: PIN-TAN

  Hier werden bei Verwendung des PIN/TAN-Verfahrens PIN und TAN eingestellt. Bei der Verwendung anderer Sicherheitsverfahren muss die DEG nicht belegt werden. Ihr Inhalt wird in diesem Fall ignoriert.

  Details siehe VI.5.3.1

- **Beispiel**

```
HNSHA:8:1+654321+@96@<Signatur>'

HNSHA:8:1+654321++8342:954378'
```

VI.5.3.1 PIN-TAN

- **Beschreibung**

  Enthält im Falle des PIN/TAN-Verfahrens die PIN und evtl. eine TAN. Die PIN ist in jeder Nachricht zu senden. Ob eine TAN erforderlich ist, hängt von den im DIPINS-Segment festgelegten Anforderungen der Geschäftsvorfälle ab.

- **Format**

  Name: PIN/TAN
  Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	PIN	GD	an	..6	M	1	
2	TAN	GD	an	..35	K	1	

- **Erläuterungen**

  Nr. 1: PIN

  Spezifiziert die PIN.

  Nr. 2: TAN

  Spezifiziert die TAN.

- **Beispiel**

```
8342:954378
```

VI.5.4 Verschlüsselungskopf

VI.5.4.1 Segmentbeschreibung

♦ **Beschreibung**

Der Verschlüsselungskopf enthält Informationen über die Art des Sicherheitsservice, die Verschlüsselungsfunktion und die zu verwendenden Chiffrierschlüssel.

Zum Abgleich mit den in den BPD definierten Verschlüsselungsverfahren DDV bzw. RDH wird das Feld „Bezeichner für Algorithmusparameter, Schlüssel“ herangezogen (vgl. Kap. VI.5.4.2).

♦ **Format**

Name: Verschlüsselungskopf
Typ: Segment
Segmentart: Administration
Kennung: HNVSK
Bezugssegment: -
Segmentversion: 2
Sender: Kunde/Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Sicherheitsfunktion, kodiert	DE	an	..3	M	1	4, 998
3	Rolle des Sicherheitslieferanten, kodiert	DE	an	..3	M	1	1, 4
4	Sicherheitsidentifikation, Details	DEG			M	1	
5	Sicherheitsdatum und –uhrzeit	DEG			M	1	
6	Verschlüsselungs-algorithmus	DEG			M	1	
7	Schlüsselname	DEG			M	1	
8	Komprimierungsfunktion	DE	an	..3	M	1	0
9	Zertifikat	DEG			K	1	

♦ **Erläuterungen**

Nr. 2: Sicherheitsfunktion, kodiert

Spezifiziert die auf die Nachricht angewendete Sicherheitsfunktion.

Im Zusammenhang mit Verschlüsselung und Komprimierung ist momentan nur folgender Wert möglich:

- "4" für ENC, Encryption (Verschlüsselung und evtl. Komprimierung)
- „998“, Klartext

Nr. 3: Rolle des Sicherheitslieferanten, kodiert

Beschreibt das Verhältnis desjenigen, der die Sicherheit gewährleistet bezüglich der zu sichernden Nachricht.

Es sind folgende Werte möglich:

- "1" für ISS, Herausgeber der chiffrierten Nachricht (Erfasser)
- "4" für WIT, der Unterzeichnete ist Zeuge, aber für den Inhalt der Nachricht nicht verantwortlich (Übermittler, welcher nicht Erfasser ist).

Nr. 4: Sicherheitsidentifikation, Details

Identifikation der im Sicherheitsprozess involvierten Parteien. Dient zur Übermittlung der CID im DDV-Verfahren bzw. der Kundensystem-ID im RDH-Verfahren.

Details siehe VI.5.1.3

Nr. 5: Sicherheitsdatum und -uhrzeit

Zeitstempel, der anzeigt, wann die Sicherheitsfunktion angewendet wurde. Als Bedeutung wird „1“ eingestellt, da es sich um einen Sicherheitszeitstempel handelt.

Details siehe VI.5.1.2

Nr. 6: Verschlüsselungsalgorithmus

Enthält einen kryptographischen Algorithmus, seinen Operationsmodus, so wie dessen Einsatz, in diesem Fall den verschlüsselten Nachrichtenschlüssel und den Initialisierungsvektor.

Details siehe VI.5.4.2

Nr. 7: Schlüsselname

Enthält den verwendeten Schlüsselnamen, respektive die Referenz auf den Chiffrierschlüssel.

Details siehe VI.5.1.1

Nr. 8: Komprimierungsfunktion

Für die verschiedenen Komprimierungsverfahren sind folgende Werte vorgesehen:

Code	Bedeutung	Erläuterung
0	NULL	keine Kompression[9]
1	LZW	Lempel, Ziv, Welch
2	COM	optimized LZW
3	LZSS	Lempel, Ziv
4	LZHuf	LZ + Huffman Coding
5	ZIP	PKZIP
999	ZZZ	gegenseitig vereinbart

Nr. 9: Zertifikat

Hier wird bei späterem Einsatz von Zertifizierungsinstanzen ein Zertifikat transparent eingestellt.

Details siehe VI.5.1.4

[9] Z.Zt. wird nur der Wert „0“ für „keine Kompression“ unterstützt.

- **Beispiel**

```
HNVSK:998:2+4+1+1::1+1:19960610:102044+2:2:13:@9
6@<chiffrierter Schlüssel>:6:1+280:10020030:1234
5:V:1:1+0'
```

VI.5.4.2 Verschlüsselungsalgorithmus

♦ **Beschreibung**

Enthält einen kryptographischen Algorithmus, seinen Operationsmodus, so wie dessen Einsatz.

♦ **Format**

Name: Verschlüsselungsalgorithmus
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Verwendung des Verschlüsselungsalgorithmus, kodiert	GD	an	..3	M	1	2
2	Operationsmodus, kodiert	GD	an	..3	M	1	2
3	Verschlüsselungsalgorithmus, kodiert	GD	an	..3	M	1	13
4	Wert des Algorithmusparameters, Schlüssel	GD	bin	..512	M	1	
5	Bezeichner für Algorithmusparameter, Schlüssel	GD	an	..3	M	1	5,6
6	Bezeichner für Algorithmusparameter, IV	GD	an	..3	M	1	1
7	Wert des Algorithmusparameters, IV	GD	bin	..512	K	1	

♦ **Erläuterungen**

Nr. 1: Verwendung des Verschlüsselungsalgorithmus, kodiert

Spezifiziert die Verwendung des in Feld 2 identifizierten Algorithmus.

Im Zusammenhang mit der Verschlüsselung sind derzeit folgende Werte möglich:

- "2" für OSY, Owner Symmetric

Nr. 2: Operationsmodus, kodiert

Spezifiziert den verwendeten Operationsmodus:

- "2" für CBC, Cipher Block Chaining.

Nr. 3: Verschlüsselungsalgorithmus, kodiert

Spezifiziert den verwendeten Verschlüsselungsalgorithmus:

- "13" für 2-Key-Triple-DES

Nr. 4: Wert des Algorithmusparameters, Schlüssel

Dieser Algorithmusparameter enthält den verschlüsselten Nachrichtenschlüssel, welcher im Feld " Wert des Algorithmusparameters, Schlüssel" steht.

Beim PIN/TAN-Verfahren wird als PIN/TAN-Default z.B.
X'00 00 00 00 00 00 00 00' verwendet.

Nr. 5: Bezeichner für Algorithmusparameter, Schlüssel

Das Feld enthält die genaue Eigenschaft für die beiden Verfahren DDV und RDH (Die Steuerung erfolgt in den BPD, vgl. Kapitel IV.4). Es werden in HBCI folgende Werte verwendet:

- „5“ für KYE, Symmetrischer Schlüssel, ver- bzw. entschlüsselt mit einem symmetrischen Schlüssel bei DDV (vgl. Kapitel VI.2.2.1).
- „6“ für KYP, Symmetrischer Schlüssel, verschlüsselt mit einem öffentlichen Schlüssel bei RDH.

Beim PIN/TAN-Verfahren wird als PIN/TAN-Default z.B. „5“ verwendet.

Nr. 6: Bezeichner für Algorithmusparameter, IV

- "1" für IVC, Initialization value, clear text

Nr. 7: Wert des Algorithmusparameters, IV

Es wird folgender Initialisierungswert als Default verwendet:

X’00 00 00 00 00 00 00 00’

In einer zukünftigen Version kann dieses DE mit einem abweichenden Initialisierungswert belegt werden. Zur Zeit ist die Belegung nicht zulässig (gilt auch für das PIN/TAN-Verfahren).

♦ **Beispiel**

```
2:2:13:@96@<chiffrierter Schlüssel>:6:1
```

VI.5.5 Verschlüsselte Daten

- **Beschreibung**

  Dieses Segment enthält die verschlüsselten (und komprimierten) Daten.

- **Format**

  Name: Verschlüsselte Daten
  Typ: Segment
  Segmentart: Administration
  Kennung: HNVSD
  Bezugssegment: -
  Segmentversion: 1
  Sender: Kunde/Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Daten, verschlüsselt	DE	bin	..	M	1	

- **Erläuterungen**

  Nr. 2: Daten, verschlüsselt

  Enthält die verschlüsselten (und komprimierten) Daten, beim PIN/TAN-Verfahren die unverschlüsselten Daten (die Verschlüsselung erfolgt hier via Transportverschlüsselung des verwendeten Transportprotokolls HTTPS).

- **Beispiel**

```
HNVSD:999:1+@348@<Daten, un/verschlüsselt>'
```

VI.6 PIN/TAN Management

Bei Verwendung des PIN/TAN-Verfahrens werden einige Geschäftsvorfälle benötigt, um z.B. eine PIN zu ändern, eine neue TAN-Liste anzufordern oder eine PIN bzw. eine TAN-Liste zu sperren.

Alle Geschäftsvorfälle zum PIN/TAN-Management werden innerhalb eines personalisierten Dialoges gesendet, also nach Eingabe der PIN. Falls zusätzlich eine TAN erforderlich ist, ist dies in der Beschreibung des Geschäftsvorfalls vermerkt. PIN und TAN werden in die entsprechenden Felder des Signaturabschlusses eingestellt (vgl. Kapitel VI.5.3) und sind im Geschäftsvorfall selbst nicht vorhanden.

Die Geschäftsvorfälle zum PIN/TAN-Management sollten vom Kundenprodukt immer in einem geschlossenen Kontext, d.h. in separaten Nachrichten in einem separaten Dialog 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. Des weiteren ist vom Kundenprodukt sicherzustellen, dass eine HBCI-Nachricht entweder nur einen einzelnen Geschäftsvorfall enthält, für den eine TAN erforderlich ist, oder nur solche Geschäftsvorfälle, für die keine TAN erforderlich ist. Andernfalls ist die eindeutige Zuordnung der übergebenen TAN zu den Geschäftsvorfällen nicht sichergestellt.

Eine Mischung von Geschäftsvorfällen, die eine TAN erfordern, mit solchen, die keine erfordern, ist generell nicht zulässig.

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

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:

Code	Beispiel für Rückmeldungstext
3910	TAN wurde nicht verbraucht.
3911	Bitte neue TAN-Liste aktivieren.
3913	TAN wurde verbraucht
9931	Teilnehmersperre durchgeführt
9932	PIN muss zwangsweise geändert werden.
9941	TAN ungültig
9942	PIN ungültig
9991	TAN bereits verbraucht

Damit der Kunde 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 Kunden die gleiche TAN noch einmal verwendet werden.

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

VI.6.1 Verwalten von PIN und TAN-Listen

VI.6.1.1 PIN-Änderung

Dieser Geschäftsvorfall bewirkt das Ändern der PIN. Zum Ändern der PIN ist im Signaturabschluss 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 Institut vergebene PIN durch eine persönliche PIN zu ersetzen.
- Auf Wunsch des Kunden
- Zwangsänderung bei Verdacht auf Kompromittierung

Realisierung Bank: optional
Realisierung Kunde: optional

a) Kundenauftrag

♦ **Format**

Name: PIN ändern
Typ: Segment
Segmentart: Administration
Kennung: DKPAE
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Neue PIN	DE	an	..6	K	1	

♦ **Beispiel**

```
DKPAE:4:1+04321'
```

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

- **Format**

Name:	PIN ändern Parameter
Typ:	Segment
Segmentart:	Geschäftsvorfall
Kennung:	DIPAES
Bezugssegment:	HKVVB
Segmentversion:	1
Sender:	Kreditinstitut
Format:	Geschäftsvorfall ohne Parameter

- **Erläuterungen**

  Geschäftsvorfallspezifische Parameter existieren nicht.

  Nr. 4: Parameter

  Die DEG wird nicht belegt.

- **Beispiel**

```
DIPAES:4:1:5+1+1'
```

VI.6.1.2 TAN-Liste anfordern

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

Realisierung Bank: optional
Realisierung Kunde: optional

a) Kundenauftrag

- **Format**

Name: TAN-Liste anfordern
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: DKTLA
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

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

- **Erläuterungen**

Abhängig vom Verfahren des Kreditinstitutes muss / kann der Kunde eine neue TAN-Liste anfordern oder bekommt diese automatisch zugesendet.

- **Beispiel**

```
DKTLA:4:1'
```

b) Kreditinstitutsrückmeldung

- **Erläuterungen**

Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen

c) Bankparameterdaten

- **Format**

Name: TAN-Liste anfordern Parameter
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: DITLAS
Bezugssegment: HKVVB
Segmentversion: 1
Sender: Kreditinstitut
Format: Geschäftsvorfall ohne Parameter

- **Erläuterungen**

Geschäftsvorfallspezifische Parameter existieren nicht.

Nr. 4: Parameter

Die DEG wird nicht belegt.

- **Beispiel**

```
DITLAS:4:1:5+1+2'
```

VI.6.1.3 TAN-Liste freischalten

Dieses Segment bewirkt das Freischalten einer TAN-Liste.

Zum Aktivieren der neuen TAN-Liste gibt es verschiedene Verfahren, z.B.: es ist eine Transaktionsnummer der alten Liste und eine Transaktionsnummer der neuen Liste dem Institut zu übermitteln. Die TAN der alten Liste wird in den Signaturabschluss eingestellt.

Realisierung Bank: optional
Realisierung Kunde: optional

a) Kundenauftrag

- **Format**

Name: TAN-Liste freischalten
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: DKTLF
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	neue TAN	DE	an	..35	M	1	
3	TAN-Listennummer	DE	num	..8	K	1	

- **Erläuterungen**

Nr. 2: neue TAN

Eine TAN der neuen freizuschaltenden Liste.

Nr. 3: TAN-Listennummer

Jede TAN-Liste hat eine eigene Nummer, welche sie eindeutig identifiziert. Hier kann die Nummer der TAN-Liste eingestellt werden, die freigeschaltet werden soll. Die verbleibenden TANs einer vorher aktiven Liste werden ungültig.

- **Beispiel**

```
DKTLF:4:1+4711+1'
```

b) Kreditinstitutsrückmeldung

- **Erläuterungen**

Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	TAN-Liste Nr. xxx aktiviert

c) Bankparameterdaten

♦ Format

Name: TAN-Liste freischalten Parameter
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: DITLFS
Bezugssegment: HKVVB
Segmentversion: 1
Sender: Kreditinstitut
Format: Geschäftsvorfall mit Parametern

♦ Erläuterungen

Name: Parameter TAN-Liste freischalten
Typ: Datenelementgruppe
Status: M

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	TAN-Listennummer erforderlich	GD	jn	#	M	1	

Nr. 1 : TAN-Listennummer erforderlich

Abhängig vom Kreditinstitut ist die TAN-Listennummer bei deren Freischaltung anzugeben oder nicht. Ist deren Angabe nicht erforderlich, können vom Kunden dennoch eingestellte TAN-Listennummern vom Kreditinstitut ignoriert werden.

♦ Beispiel

```
DITLFS:4:1:5+1+2+N'
```

VI.6.2 Sperren von PIN bzw. TAN-Listen

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.

Bei jedem Erhalt einer falsch signierten Nachricht für einen noch nicht gesperrten Benutzer wird der jeweilige Fehlbedienungszähler (PIN oder TAN) erhöht. Nach Überschreiten des vom Kreditinstitut vorgegebenen Wertes wird eine Sperre vorgenommen.

Hierbei ist zu unterscheiden, dass die Eingabe fehlerhafter TANs zu einer Teilnehmersperre und fehlerhafte PINs zu einer Kontosperre führen.

Abhängig vom Kreditinstitut können vorliegende Sperren entweder vom Kunden selbst oder nur durch das Kreditinstitut aufgehoben werden.

VI.6.2.1 PIN-Sperre

Dieser Geschäftsvorfall bewirkt das Sperren des Online-Zugangs. Diese Sperre kann durch den Geschäftsvorfall „PIN-Sperre aufheben“ wieder rückgängig gemacht werden.

Realisierung Bank: optional
Realisierung Kunde: optional

a) Kundenauftrag

- **Format**

Name: PIN sperren
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: DKPSP
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

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

- **Erläuterungen**

Der Signaturabschluss muss eine gültige PIN enthalten.

- **Beispiel**

```
DKPSP:4:1'
```

b) Kreditinstitutsrückmeldung

- **Erläuterungen**

Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	PIN-Sperre erfolgreich

c) Bankparameterdaten

- **Format**

Name: PIN sperren Parameter
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: DIPSPS
Bezugssegment: HKVVB
Segmentversion: 1
Sender: Kreditinstitut
Format: Geschäftsvorfall ohne Parameter

- **Erläuterungen**

Geschäftsvorfallspezifische Parameter existieren nicht.

Nr. 4: Parameter

Die DEG wird nicht belegt.

- **Beispiel**

```
DIPSPS:4:1:5+1+2'
```

VI.6.2.2 PIN-Sperre aufheben

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 Signaturabschluss).

Da bei gesperrter PIN im Regelfall kein weiterer Dialog möglich ist, da bereits die Dialoginitialisierung abgelehnt wird, kann dieser Geschäftsvorfall nur angeboten werden, wenn das Kreditinstitut nach einer PIN-Sperre einen weiteren Dialog mit der gesperrten PIN zulässt, sofern in diesem nur der Geschäftsvorfall „PIN-Sperre aufheben“ gesendet wird.

Realisierung Bank: optional
Realisierung Kunde: optional

a) Kundenauftrag

- **Format**

Name: PIN-Sperre aufheben
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: DKPSA
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

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

- **Beispiel**

```
DKPSA:4:1'
```

b) Kreditinstitutsrückmeldung

- **Erläuterungen**

Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	PIN-Sperre aufgehoben

c) Bankparameterdaten

- **Format**

Name:	PIN-Sperre aufheben Parameter
Typ:	Segment
Segmentart:	Geschäftsvorfall
Kennung:	DIPSAS
Bezugssegment:	HKVVB
Segmentversion:	1
Sender:	Kreditinstitut
Format:	Geschäftsvorfall ohne Parameter

- **Erläuterungen**

Geschäftsvorfallspezifische Parameter existieren nicht.

Nr. 4: Parameter

Die DEG wird nicht belegt.

- **Beispiel**

```
DIPSAS:4:1:5+1+2'
```

VI.6.2.3 TAN-Liste sperren

Dieses Segment bewirkt das Sperren der TAN-Liste. Diese Sperre kann je nach Institut vom Mitarbeiter wieder rückgängig gemacht werden.

Realisierung Bank: optional
Realisierung Kunde: optional

a) Kundenauftrag

- **Format**

Name: TAN-Liste sperren
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: DKTSP
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	TAN-Listennummer	DE	num	..8	K	1	

- **Erläuterungen**

Nr. 2: TAN-Listennummer

Jede TAN-Liste hat eine eigene Nummer, welche sie eindeutig identifiziert. Hier kann die Nummer der TAN-Liste eingestellt werden, die gesperrt werden soll.

- **Beispiel**

```
DKTSP:4:1'
```

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
3914	neue TAN-Liste aktivieren
3915	neue TAN-Liste aktiviert

c) Bankparameterdaten

- **Format**

Name: TAN-Liste sperren Parameter
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: DITSPS
Bezugssegment: HKVVB
Segmentversion: 1
Sender: Kreditinstitut
Format: Geschäftsvorfall mit Parametern

- **Erläuterungen**

Name: Parameter TAN-Liste sperren
Typ: Datenelementgruppe
Status: M

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	TAN-Listennummer erforderlich	GD	jn	#	M	1	

Nr. 1 : TAN-Listennummer erforderlich

Abhängig vom Kreditinstitut ist die TAN-Listennummer bei deren Sperrung anzugeben oder nicht. Ist deren Angabe nicht erforderlich, können vom Kunden dennoch eingestellte TAN-Listennummern vom Kreditinstitut ignoriert werden.

- **Beispiel**

```
DITSPS:4:1:5+1+2+N'
```

VI.6.2.4 TAN-Liste anzeigen

Dieses Segment bewirkt die Anzeige der verbrauchten TANs des Kunden.

Realisierung Bank: optional
Realisierung Kunde: optional

a) Kundenauftrag

- **Format**

Name: TAN-Liste anzeigen
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: DKTAZ
Bezugssegment: -
Segmentversion: 1
Sender: Kunde

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

- **Erläuterungen**

Das Auftragssegment enthält neben dem Segmentkopf keine weiteren Daten.

- **Beispiel**

```
DKTAZ:4:1'
```

b) Kreditinstitutsrückmeldung

- **Format**

Name: TAN-Liste
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: DITAZ
Bezugssegment: DKTAZ
Segmentversion: 1
Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Zustandskennzeichen	DE	an	1	M	1	
3	TAN-Listennummer	DE	num	..8	M	1	
4	Erstellungsdatum	DE	dat	#	K	1	
5	TAN-Information	DEG			K	999	

Je zurückzumeldender TAN-Liste ist ein DITAZ-Segment in die Antwortnachricht einzustellen.

- **Erläuterungen**

Nr. 2: Zustandskennzeichen

- A Aktive Liste
- S Sperre der Liste
- V Vorherige Liste

Nr. 3: TAN-Listennummer

Nummer der TAN-Liste, die zurückgemeldet wird.

Nr. 4: Erstellungsdatum

Datum, an dem die Liste erstellt wurde.

Nr. 5: TAN-Information

Informationen zu einer TAN der TAN-Liste.

Details siehe VI.6.2.4.2

♦ **Beispiel**

```
DITAZ:4:1+A+4711+20010102+8:TAN1:20010509:103020
+5:TAN2:20010619:114010+0+0'
```

VI.6.2.4.1 TAN-Information

Die DEG enthält die Daten zu einer TAN.

♦ **Format**

Name: TAN-Information
Typ: Datenelementgruppe

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Verbrauchskennzeichen	GD	num	1	M	1	
2	TAN	GD	an	..35	K	1	
3	Verbrauchsdatum	GD	dat	#	K	1	
4	Verbrauchsuhrzeit	GD	tim	#	K	1	

♦ **Erläuterungen**

Nr. 1: Verbrauchskennzeichen

- 0 freie TAN
- 1 Einzel/Sammelüberweisung Stornierung
- 2 PIN-Änderung
- 3 Kontosperre aufheben
- 4 Aktivieren neuer TAN-Liste
- 5 Entwertete TAN (maschinell)
- 6 Mitteilung mit TAN
- 7 PC-Übertragung (Überweisung/Lastschrift)
- 8 Wertpapierorder (Neuanlage/Änderung/Löschung)
- 9 Dauerauftrag (Neuanlage/Änderung/Löschung)

Nr. 2: TAN

TAN in Klarschrift (nur vorhanden, wenn TAN verbraucht ist)

Nr. 3: Verbrauchsdatum

nur vorhanden, wenn TAN verbraucht ist

Nr. 4: Verbrauchsuhrzeit

nur vorhanden, wenn TAN verbraucht ist

- **Beispiel**

```
8:TAN1:20010509:103020
```

a) Bankparameterdaten

- **Format**

Name:	TAN-Liste anzeigen Parameter
Typ:	Segment
Segmentart:	Geschäftsvorfall
Kennung:	DITAZS
Bezugssegment:	HKVVB
Segmentversion:	1
Sender:	Kreditinstitut
Format:	Geschäftsvorfall ohne Parameter

- **Erläuterungen**

Geschäftsvorfallspezifische Parameter existieren nicht.

Nr. 4: Parameter

Die DEG wird nicht belegt.

- **Beispiel**

```
DITAZS:4:1:5+1+2'
```

VI.6.2.5 TAN prüfen und „verbrennen“

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

- **mögliche Rückmeldungscodes**

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

VI.6.2.6 PIN prüfen

Um eine PIN prüfen zu lassen, wird dem HBCI-Benutzer kein spezieller Geschäftsvorfall bereitgestellt. Vielmehr ist diese PIN-Prüfung innerhalb der Dialoginitialisierung implizit von der Bankanwendung durchzuführen. Die PIN wird an die Bankanwendung übermittelt und kann dort geprüft werden. Die Ergebnisse der Prüfung werden von der Bankanwendung als zusätzliche Returncodes innerhalb der Initialisierungsantwort zurückgemeldet.

- **mögliche Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0901	PIN gültig
9942	PIN ungültig

VI.6.3 PIN-TAN-spezifische Erweiterungen der BPD

Für die Verwendung des PIN-TAN-Verfahrens müssen dem Kundenprodukt weitere 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.

Die hierfür notwendige BPD-Erweiterung wird in Form eines speziellen Parametersegmentes realisiert, welches sich auf keinen echten Geschäftsvorfall bezieht, sondern Daten zu allen in HBCI unterstützten Geschäftsvorfällen aufnehmen kann.

Das Spezialsegment DIPINS wird verwendet, um in die BPD-Segmentfolge PIN/TAN-spezifische Daten einzufügen. Aufgrund seines Aufbaus analog zu einem Segmentparametersegment wird es von Kundenprodukten, die das PIN/TAN-Verfahren nicht unterstützen, ignoriert, da es sich auf einen ihnen unbekannten Geschäftsvorfall zu beziehen scheint.

Die in DIPINS aufgeführten Geschäftsvorfälle dürfen vom Kunden 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-Verfahren nicht verwendet werden.

Um die Kompatibilität von HBCI mit PIN/TAN-Erweiterung und HBCI ohne PIN/TAN sicherzustellen, konnte der mögliche Wertebereich innerhalb von HISHV-Segmenten nicht um einen weiteren Wert für das PIN/TAN-Verfahren erweitert werden. Clients können diesem Segment somit nicht entnehmen, ob das PIN/TAN-Verfahren unterstützt wird oder nicht. Dies muss am Vorkommen von DIPINS-Segmenten festgemacht werden. Ist ein solches Segment vorhanden, wird PIN/TAN unterstützt, andernfalls nicht.

Realisierung Bank: verpflichtend, falls Geschäftsvorfälle mit PIN/TAN-Absicherung angeboten werden
Realisierung Kunde: optional

- **Format**

Name: BPD-Erweiterung für PIN-TAN-Verfahren
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: DIPINS
Bezugssegment: HKVVB
Segmentversion: 1
Sender: Kreditinstitut
Format: Geschäftsvorfall mit Parametern

- **Erläuterungen**

Name: Parameter BPD-Erweiterung für PIN-TAN-Verfahren
Typ: Datenelementgruppe
Status: M

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Geschäftsvorfallspezifische PIN-TAN-Informationen	GDG			K	999	

Nr. 1 : Geschäftsvorfallspezifische PIN-TAN-Informationen

Eine GDG dieses Typs enthält für genau einen Geschäftsvorfall PIN-TAN-relevante Informationen. Ist für einen Geschäftsvorfall eine zugehörige GDG hinterlegt, kann das Kundenprodukt diesen Geschäftsvorfall über das PIN-TAN-Verfahren absichern, andernfalls ist dies nicht erlaubt.

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkennung	GD	an	..6	M	1	
2	TAN erforderlich	GD	jn	#	M	1	

Nr. 1: Segmentkennung

Kennung des Geschäftsvorfalls, auf den sich die PIN-TAN- Informationen beziehen.

Nr. 2: TAN erforderlich

Es wird angegeben, ob beim Einreichen des Geschäftsvorfalles je vorhandener Signatur eine TAN angegeben werden muss oder nicht.

Hierdurch wird nicht festgelegt, ob und wie oft ein Geschäftsvorfall zu signieren ist. Dies wird weiterhin über die BPD und UPD angegeben.

Werden mehr Signaturen eingestellt als in BPD und UPD gefordert, so sind diese alle gemäß der Einstellungen im DIPINS-Segment zu bilden.

Werden in BPD und UPD keine Signaturen gefordert, können diese selbst dann weggelassen werden, wenn für den betreffenden Geschäftsvorfall eine TAN erforderlich ist.

♦ **Beispiel**

```
DIPINS:4:1:5+1+1+HKUEB:J:HKKAN:N:HKSUB:J:DKPAE:J
:DKTLF:J'
```

VI.7 PIN/TAN-Kommunikationszugänge

Für das PIN/TAN-Verfahren wird neben TCP/IP ein neuer Kommunikationszugang über HTTPS eingeführt. Um die zugehörige Kommunikationsadresse an das Kundenprodukt zurückmelden zu können, wird die gültige Belegung eines HIKOM-Segmentes wie folgt erweitert:

- **Format**

Name: Kommunikationszugang rückmelden
Typ: Segment
Segmentart: Geschäftsvorfall
Kennung: HIKOM
Bezugssegment: HKKOM
Version: 3
Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Kreditinstitutskennung	DEG	kik	#	M	1	
3	Standardsprache	DE	num	..3	M	1	1,2,3
4	Kommunikationsparameter	DEG			M	1..9	

Nr. 4: Kommunikationsparameter

Die Kommunikationsparameter enthalten Informationen für den Aufbau der Transportverbindung.

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Kommunikationsdienst	DE	num	..2	M	1	1,2,3
2	Kommunikationsadresse	DE	an	..512	M	1	
3	Kommunikationsadressenzusatz	DE	an	..512	K	1	
4	Filterfunktion	DE	an	3	K	1	MIM, UUE
5	Version der Filterfunktion	DE	num	..3	K	1	

Nr. 1: Kommunikationsdienst

Unterstütztes Kommunikationsverfahren (Protokollstack), auf das sich Nachstehendes bezieht (s. Kap. „Transportmedienspezifische Festlegungen“).

Zur Zeit unterstützte Kommunikationsverfahren:

1: T-Online (Protokollstack ETSI 300 072 (CEPT), EHKP, BtxFIF)

2: TCP/IP (Protokollstack SLIP/PPP)

3: HTTPS (für PIN/TAN-Verfahren)

Nr. 2: Kommunikationsadresse

Beim Zugang über T-Online ist die Gateway-Seite als numerischer Wert (ohne die Steuerzeichen * und #) einzustellen.

Beim Zugang über TCP/IP ist die IP-Adresse als alphanumerischer Wert (z.B. '123.123.123.123') einzustellen.

Beim Zugang über HTTPS ist die Adresse des Servlets als alphanumerischer Wert (z.B. ‚https://www.xyz.de:7000/PinTanServlet') einzustellen.

Nr. 3: Kommunikationsadressenzusatz

Beim Zugang über T-Online ist der Regionalbereich einzustellen (‚00' für ein bundesweites Angebot). Beim Zugang über TCP/IP oder HTTPS wird das Feld nicht belegt.

Nr. 4: Filterfunktion

Falls das Übertragungsverfahren eine Umwandlung der Nachricht in eine 7 Bit-Zeichendarstellung erfordert (z.B. Internet), so ist hier das anzuwendende Filterverfahren anzugeben. Die Nachricht ist stets komplett zu filtern, auch wenn eine Filterung nicht notwendig wäre, da bspw. keine binären Daten enthalten sind. Ein Kreditinstitut darf jeweils nur eine Filterfunktion unterstützen.

Codierung:

MIM: MIME Base 64

UUE: Uuencode/Uudecode

Nr. 5: Version der Filterfunktion

Version der Filterfunktion.

VI.8 Gesamtübersicht der Beispiele für Rückmeldungscodes

VI.8.1 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

VI.8.2 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

VI.8.3 Fehlermeldungen

Code	Beispiel für Rückmeldungstext
9931	Teilnehmersperre durchgeführt
9932	PIN muss zwangsweise geändert werden.
9941	TAN ungültig
9942	PIN ungültig
9942	neue PIN ungültig
9991	TAN bereits verbraucht