VI. SICHERHEIT

VI.1 Allgemeines

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

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

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

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

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

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

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

VI.2 Mechanismen

VI.2.1 Elektronische Signatur

Die Bildung der elektronischen Signatur erfolgt durch die Vorgänge

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

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

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

Realisierung Bank: optional (empfohlen)
Realisierung Kunde: optional

1. Hashing der Nachricht

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

2. Formatierung des Hashwerts

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

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

3. Berechnung der elektronischen Signatur

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

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

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

1. **Hashing der Nachricht**

   siehe „Elektronische Signatur bei DDV“

2. **Formatierung des Hashwerts**

   Die Formatierung erfolgt gemäß ISO 9796 (Kap. 5.1-5.4). Der Hashwert wird für die nachfolgende Signaturbildung als Langzahl[1] interpretiert (s. auch die Beispiele in der Anlage zu ISO 9796).

3. **Berechnung der elektronischen Signatur**

   Der Hash-Wert wird mittels RSA signiert.

VI.2.2 Verschlüsselung

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

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

Die ersten zwei Schritte sind für beide Verfahren identisch:

1. Der Sender erzeugt eine Zufallszahl als Nachrichtenschlüssel und stellt ungerade Parität sicher. Bei der Auswahl der Zufallszahl ist darauf zu achten, daß keiner der folgenden schwachen oder halbschwachen Schlüssel[2] gewählt wird (vgl. Kapitel VI.3.1.1).

   Die schwachen Schlüssel des DES-Algorithmus:

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

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

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

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).

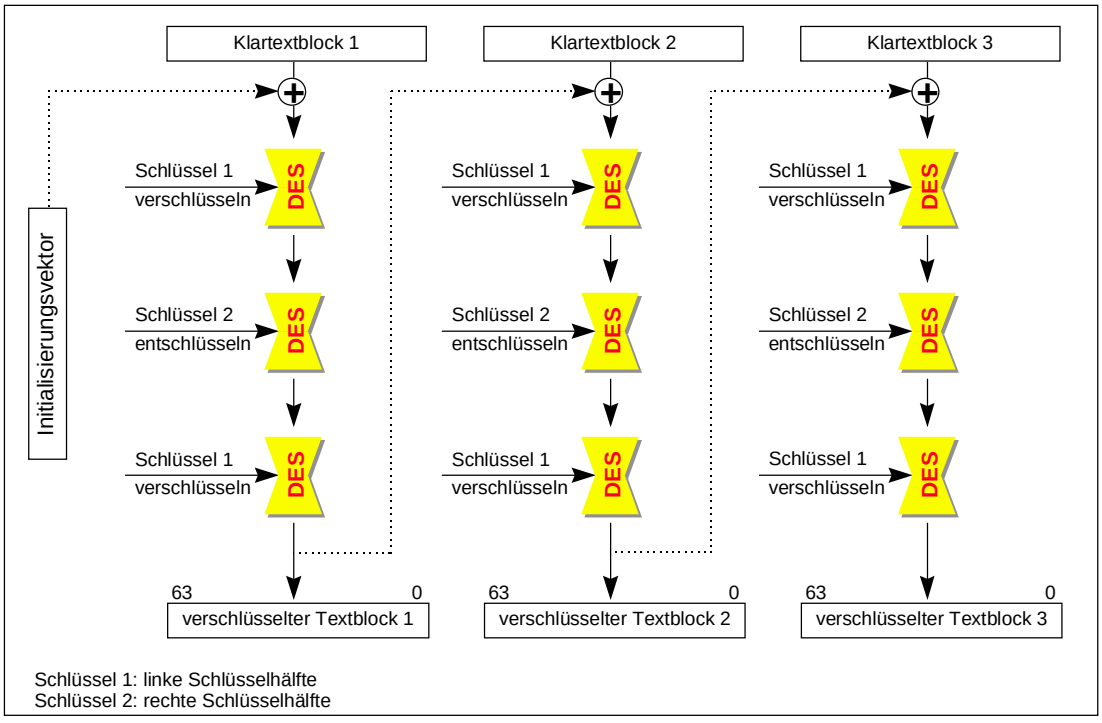

Abb. 13: 2-Key-Triple-DES im CBC-Mode

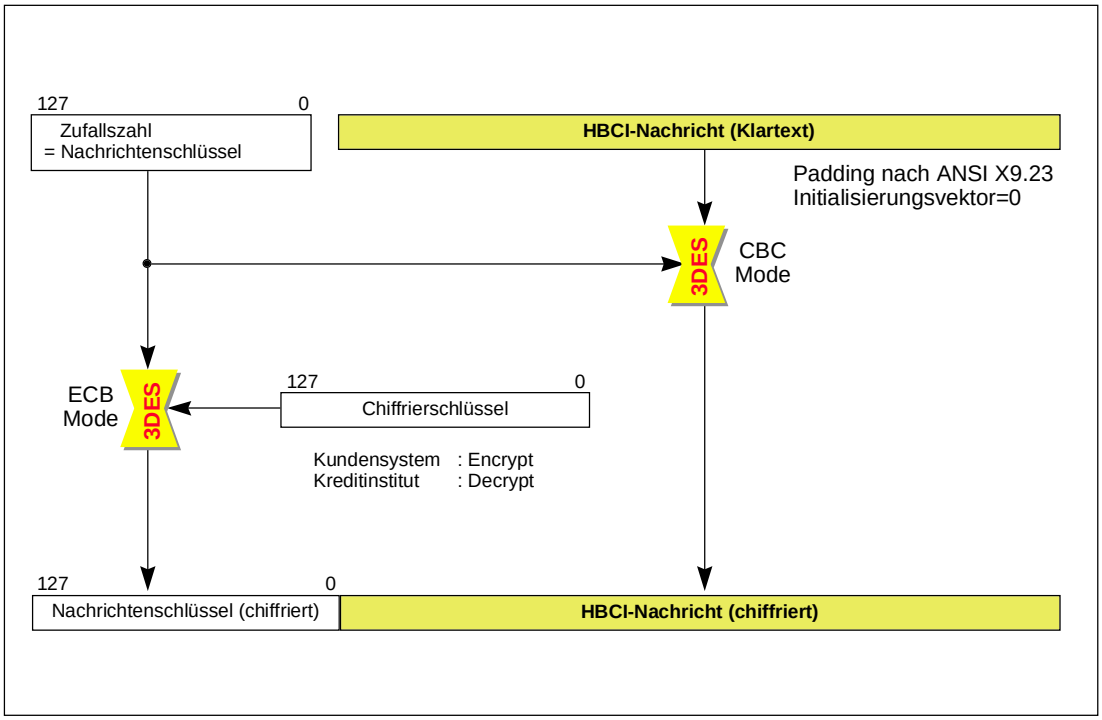

Abb. 14: Verschlüsselung bei 2-Key-Triple-DES

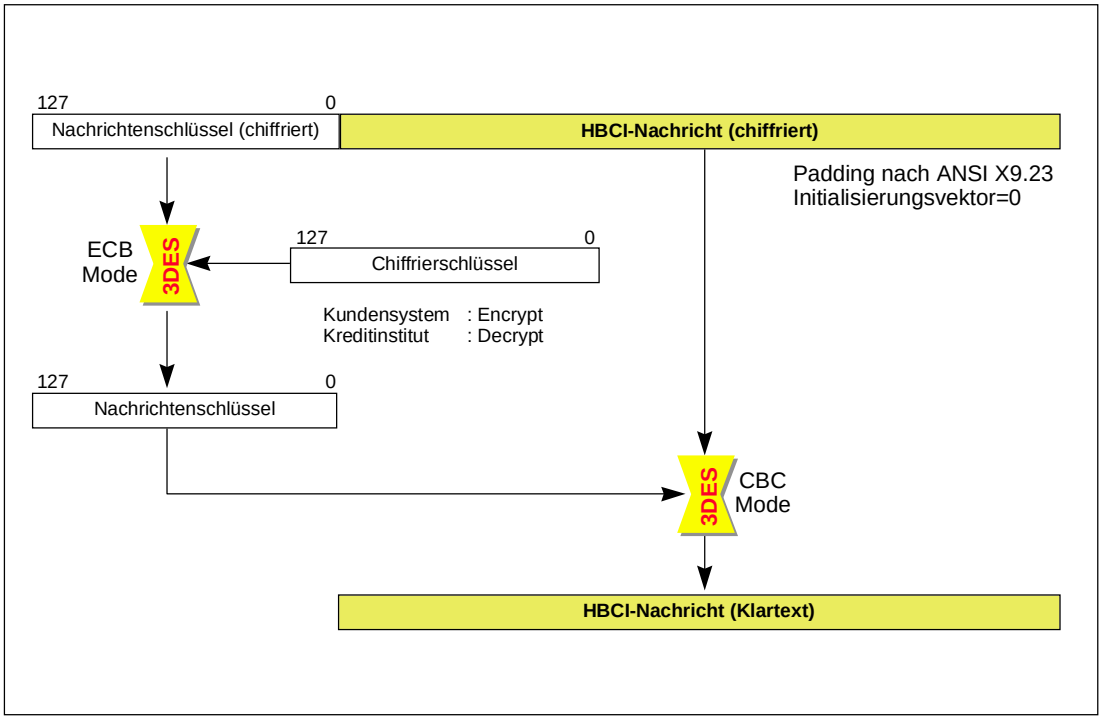

Abb. 15: Entschlüsselung bei 2-Key-Triple-DES

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.8.5.3).

Realisierung Bank: optional (empfohlen)
Realisierung Kunde: optional

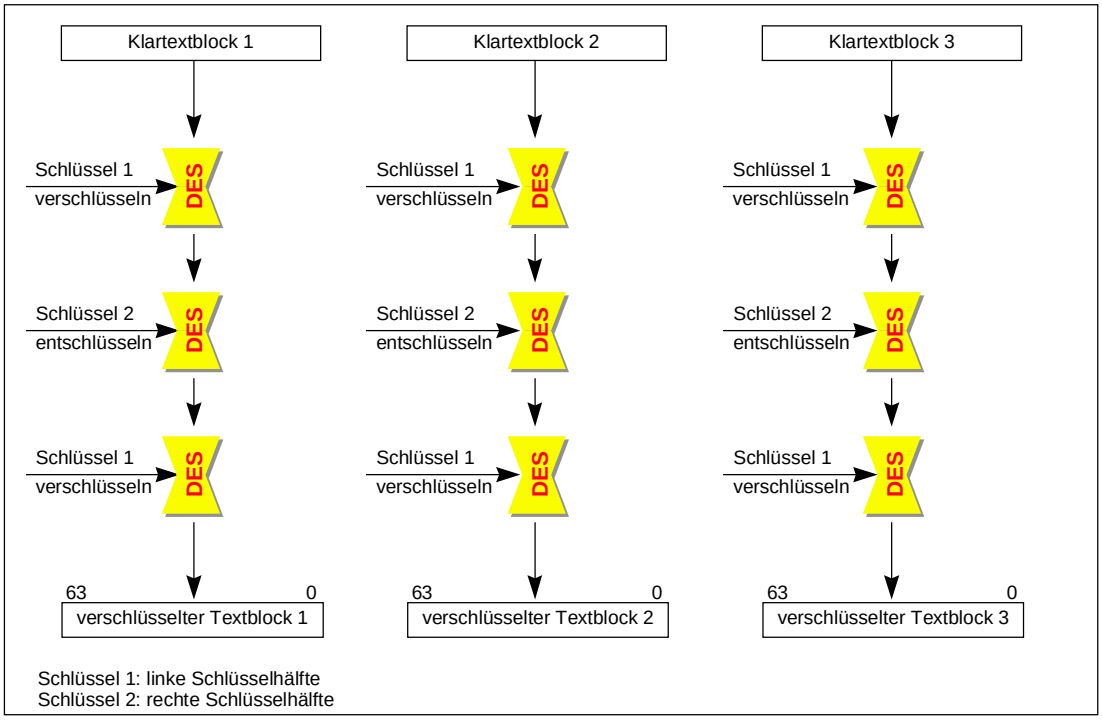

Abb. 16: 2-Key-Triple-DES im ECB-Mode

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 bzw. 24 Byte bei 3-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.

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

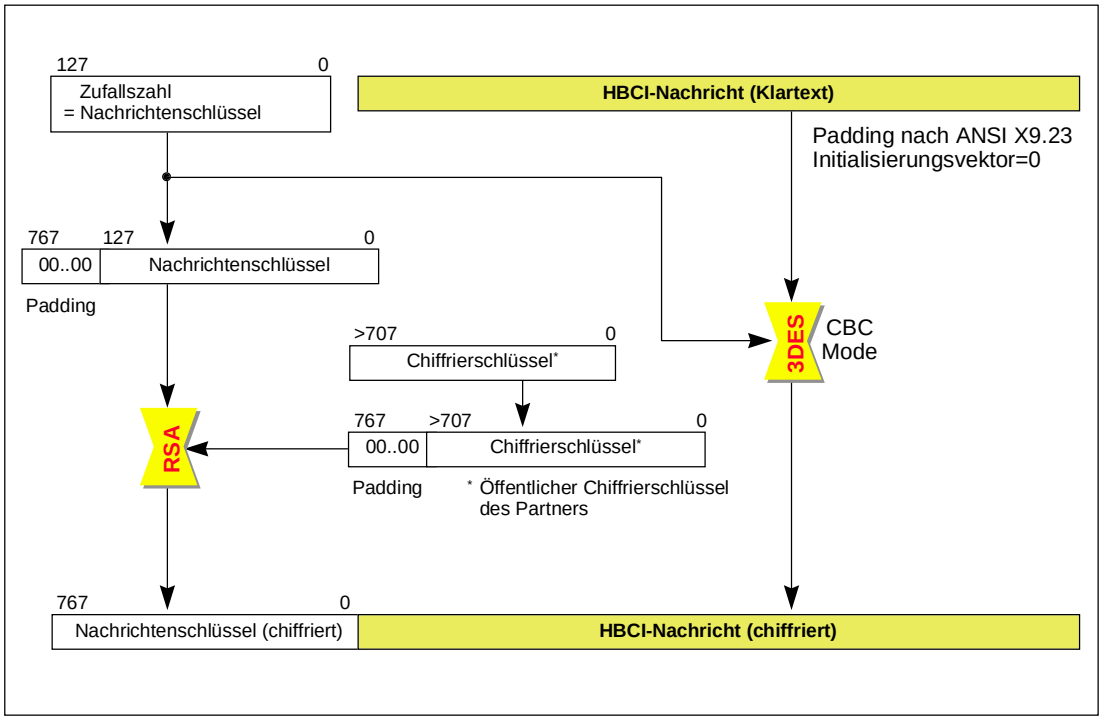

Abb. 17: Verschlüsselung bei RSA (2-Key-Triple-DES)

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.

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

VI.3 Abläufe

VI.3.1 Schlüsselverwaltung

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

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

VI.3.1.1 Gemeinsam verwendete Verfahren zur Schlüsselverwaltung

♦ **Schlüsselarten**

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

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

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

♦ **Schlüsselnamen**

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

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

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

♦ **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:[3]

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

   Die entsprechenden Forderungen werden an q gestellt.

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

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

---

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

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

VI.3.1.3.2 Initiale Schlüsselverteilung

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

- seine Benutzerkennung
- Informationen zum Kommunikationszugang

Die Übermittlung dieser Informationen ist auf zwei Wegen denkbar:

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

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

Hierzu ist folgender Ablauf vorgesehen:

1. Das Kreditinstitut übermittelt seinen öffentlichen Chiffrierschlüssel an den Kunden. Falls es Nachrichten signiert, übermittelt es ebenfalls seinen öffentlichen Signierschlüssel. Hierzu gibt es zwei Möglichkeiten:
   - Zusenden bzw. Aushändigung der Schlüssel und anderer relevanter Daten auf einem Medium (z.B. Diskette[6], Chipkarte) bei Vertragseröffnung.

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

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

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

---

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

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

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. 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.

3. 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.).

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

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

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

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

Öffentlicher Schlüssel für die elektronische Signatur:

Exponent 0768

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

Modulus 0768

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

Hash

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

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

_____ _____

Ort / Datum Unterschrift

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

VI.3.1.3.3 Schlüsseländerungen

- **Routinemäßige Schlüsseländerung des Kunden**

  Ein Kunde ändert seine Signier- und Chiffrierschlüsselpaare unabhängig.

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

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

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

- **Routinemäßige Schlüsseländerung des Kreditinstituts**

  Ein Kreditinstitut generiert bei Bedarf ein neues Schlüsselpaar.

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

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

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

VI.3.1.3.4 Schlüsselverteilung nach Kompromittierung

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

VI.3.2 Doppeleinreichungskontrolle

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

VI.3.3 Schlüsselsperrung

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

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

Zusätzlich müssen bei der Sperrung noch folgende Punkte berücksichtigt werden:

- Information des Kunden
- Entsperrung

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

♦ **Kompromittierung des eigenen Schlüssels**

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

♦ **Verlust des eigenen Schlüssels**

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

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

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

♦ **Überschreiten der Anzahl der Falschsignaturen**

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

- **Information des Kunden**

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

- **Entsperrung**

  Eine Entsperrung erfolgt nur gegen handschriftliche Unterschrift des Kunden.

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

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

VI.4 Bankfachliche Anforderungen

- **Zu signierende Nachrichten**

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

  Die Signatur von Kreditinstitutsnachrichten ist optional.

- **Doppeleinreichungskontrolle**

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

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

- **Mehrfachsignaturen**

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

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

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

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	B, S, V
4	Schlüsselnummer	GD	num	..3	M	1	
5	Schlüsselversion	GD	num	..3	M	1	

♦ **Erläuterungen**

Nr. 1: Kreditinstitutskennung

In diesem „mehrfach verwendeten HBCI-Element“ werden 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 nicht einer anderen gültigen Benutzerkennung des Kreditinstituts entsprechen.

Nr. 3: Schlüsselart

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

Abhängig vom Verwendungszweck kann die Schlüsselart drei Werte annehmen:

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

Nr. 4: Schlüsselnummer

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

Nr. 5: Schlüsselversion

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

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

Identifikation des verwendeten Schlüssels (CID, EF_ID) für DDV. Bei Verwendung des DDV-Verfahrens ist die Belegung zwingend erforderlich, bei RDH darf das Feld nicht belegt werden.

Nr. 3: Identifizierung der Partei

Code, welcher die Partei identifiziert. Bei Verwendung des RDH-Verfahrens ist die Kundensystem-ID einzustellen, sofern diese verwendet wird. Bei DDV darf das Feld nicht belegt werden.

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 Information über den damit verbundenen Sicherheitsservice, sowie über den Absender.

♦ **Format**

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

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

♦ **Erläuterungen**

Nr. 2: Sicherheitsfunktion, kodiert

Spezifiziert die auf die Nachricht angewendete Sicherheitsfunktion.

Im Zusammenhang mit elektronischen Signaturen sind folgende Werte möglich:

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

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.

Nr. 6: Sicherheitsidentifikation, Details

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

Details siehe VI.5.1.3

Nr. 7: Sicherheitsreferenznummer

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

Bei chipkartenbasierten Verfahren ist der Sequenzzähler der Chipkarte (s. Kap. VIII.8.2.9) einzustellen. Bei softwarebasierten Verfahren wird die Si-

cherheitsreferenznummer auf Basis der Kundensystem-ID und des Schlüsselnamens (Benutzerkennung) verwaltet.

Nr. 8: Sicherheitsdatum und -uhrzeit

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

Details siehe VI.5.1.2

Nr. 9: Hashalgorithmus

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

Details siehe VI.5.2.2

Nr. 10: Signaturalgorithmus

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

Details siehe VI.5.2.3

Nr. 11: Schlüsselname

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

Details siehe VI.5.1.1

Nr. 12: Zertifikat

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

Details siehe VI.5.1.4

♦ **Beispiel**

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

VI.5.2.2 Hashalgorithmus

♦ **Beschreibung**

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

♦ **Format**

Name: Hashalgorithmus
Typ: Datenelementgruppe

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

♦ **Erläuterungen**

Nr. 1: Verwendung des Hashalgorithmus, kodiert

Spezifiziert die Verwendung des in Feld 2 identifizierten Algorithmus.

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

- "1" für OHA, Owner Hashing

Nr. 2: Hashalgorithmus, kodiert

Spezifiziert den verwendeten Hash-Algorithmus:

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

Nr. 3: Bezeichner für Hashalgorithmusparameter

Dies bedingt den folgenden Wert:

- "1" für IVC, Initialization value, cleartext

Nr. 4: Wert des Hashalgorithmusparameters

Bei RIPEMD-160 wird folgender Initialisierungswert als Default verwendet: X'67 45 23 01 EF CD AB 89 98 BA DC FE 10 32 54 76 C3 D2 E1 F0'.

In einer zukünftigen Version kann dieses DE mit einem abweichenden Initialisierungswert belegt werden. Zur Zeit ist die Belegung nicht zulässig.

♦ **Beispiel**

```
1:999:1
```

VI.5.2.3 Signaturalgorithmus

♦ **Beschreibung**

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

♦ **Format**

Name: Signaturalgorithmus
Typ: Datenelementgruppe

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

♦ **Erläuterungen**

Nr. 1: Verwendung des Signaturalgorithmus, kodiert

Spezifiziert die Verwendung des in Feld 2 identifizierten Algorithmus.

Im Zusammenhang mit Signaturbildung ist derzeit nur folgender Wert möglich:

- "6" für OSG, Owner Signing

Nr. 2: Signaturalgorithmus, kodiert

Verfahren bezogen auf die Verwendung der Signatur.

Es sind folgende Werte vorgesehen:

- "1" für DES (bei DDV)
- "10" für RSA (bei RDH)

Nr. 3: Operationsmodus, kodiert

Spezifiziert den verwendeten Operationsmodus.

Es sind folgende Werte vorgesehen (vgl. Kapitel VI.2.1):

- "16" für DSMR, Digital Signature Scheme giving Message Recovery: ISO 9796 (bei RDH)
- "999" für ZZZ, gegenseitig vereinbart (bei DDV bedeutet dies die Bildung eines Retail-MAC für die Berechnung der Signatur)

♦ **Beispiel**

```
6:10:16
```

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	M	1	

♦ Erläuterungen

Nr. 2: Sicherheitskontrollreferenz

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

Nr. 3: Validierungsresultat

Enthält die elektronische Signatur.

♦ Beispiel

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

VI.5.4 Verschlüsselungskopf

VI.5.4.1 Segmentbeschreibung

♦ **Beschreibung**

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

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

♦ **Format**

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

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Sicherheitsfunktion, kodiert	DE	an	..3	M	1	4
3	Rolle des Sicherheitslieferanten, kodiert	DE	an	..3	M	1	1, 4
4	Sicherheitsidentifikation, Details	DEG			M	1	
5	Sicherheitsdatum und -uhrzeit	DEG			M	1	
6	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)

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:

- "0" für NULL, keine Kompression [7]
- "1" für LZW, Lempel, Ziv, Welch
- "2" für COM, optimized LZW
- "3" für LZSS, Lempel, Ziv
- "4" für LZHuf, LZ + Huffman Coding
- "5" für ZIP, PKZIP
- "999" für ZZZ, gegenseitig vereinbart

Nr. 9: Zertifikat

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

Details siehe VI.5.1.4

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

♦ **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.

Nr. 5: Bezeichner für Algorithmusparameter, Schlüssel

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

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

Nr. 6: Bezeichner für Algorithmusparameter, IV

- "1" für IVC, Initialization value, cleartext

Nr. 7: Wert des Algorithmusparameters, IV

Es wird folgender Initialisierungswert als Default verwendet:

X’00 00 00 00 00 00 00 00’.

In einer zukünftigen Version kann dieses DE mit einem abweichenden Initialisierungswert belegt werden. Zur Zeit ist die Belegung nicht zulässig.

♦ **Beispiel**

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

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.

♦ Beispiel

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

VI.6 Key-Management

VI.6.1 Formate für Key-Management

Für die Schlüsseländerung, die Schlüsselverteilung sowie die Schlüsselsperrung sind die nachfolgenden Segmente vorgesehen. Diese dürfen nur im Rahmen der speziellen Key-Management-Nachrichten verwendet werden.

VI.6.1.1 Änderung eines öffentlichen Schlüssels

♦ **Beschreibung**

Dieses Segment enthält einen neuen öffentlichen Schlüssel des Kunden.

♦ **Format**

Name: Schlüsseländerung
Typ: Segment
Segmentart: Administration
Kennung: HKSAK
Bezugssegment: -
Segmentversion: 2
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Nachrichtenbeziehung, kodiert	DE	num	1	M	1	2
3	Bezeichner für Funktionstyp	DE	num	..3	M	1	112
4	Schlüsselname	DEG			M	1	
5	Öffentlicher Schlüssel	DEG			M	1	
6	Zertifikat	DEG			K	1	

♦ **Erläuterungen**

Nr. 2: Nachrichtenbeziehung, kodiert

Im Zusammenhang mit der Schlüsseländerung ist immer folgender Wert vorgesehen:

- "2" für ‘Key-Management-Nachricht erwartet Antwort’

Nr. 3: Bezeichner für Funktionstyp

Im Zusammenhang mit der Schlüsseländerung ist folgender Wert vorgesehen:

- "112" für ‘Certificate Replacement’ (Ersatz des Zertifikats)

Nr. 4: Schlüsselname

Es ist der neue öffentliche Schlüssel des Kunden einzustellen. Als Schlüsselart darf nicht ‘B’ eingestellt werden, da in einem Auftragssegment nur ein Schlüssel übertragen werden kann.

Details siehe VI.5.1.1

Nr. 5: Öffentlicher Schlüssel

Datenelementgruppe zur Aufnahme des neuen öffentlichen Schlüssels des Kunden.

Details siehe VI.5.1.5

Nr. 6: Zertifikat

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

Details siehe VI.5.1.4

♦ **Beispiel**

```
HKSAK:8:2+2+112+280:10020030:12345:S:1:1+6:16:10
:@12@<Modulus>:12:@3@<Exponent>:13'
```

VI.6.1.2 Anforderung eines öffentlichen Schlüssels

♦ **Beschreibung**

Dieses Segment enthält die Anfrage nach einem öffentlichen Schlüssel des Kreditinstituts. Das Segment wird entweder innerhalb der Dialoginitialisierung (vgl. Kapitel III.3.1) oder im Rahmen der erstmaligen Schlüsselanforderung (vgl. Kapitel VI.6.2.2) gesendet.

♦ **Format**

Name: Anforderung eines öffentlichen Schlüssels
Typ: Segment
Segmentart: Administration
Kennung: HKISA
Bezugssegment: -
Segmentversion: 2
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Nachrichtenbeziehung, kodiert	DE	num	1	M	1	2
3	Bezeichner für Funktionstyp	DE	num	..3	M	1	124
4	Schlüsselname	DEG			M	1	
5	Zertifikat	DEG			K	1	

♦ **Erläuterungen**

Nr. 2: Nachrichtenbeziehung, kodiert

Im Zusammenhang mit der Anfrage nach einem öffentlichen Schlüssel ist immer folgender Wert vorgesehen:

- "2" für ‘Key-Management-Nachricht erwartet Antwort’

Nr. 3: Bezeichner für Funktionstyp

Im Zusammenhang mit der Anfrage für einen öffentlichen Schlüssel ist folgender Wert vorgesehen:

- "124" für ‘Certificate Status Request’

Nr. 4: Schlüsselname

In den Schlüsselnamen ist die Schlüsselnummer und -version des Schlüssels einzustellen, den das Kundenprodukt als aktuellen öffentlichen Schlüssel des Kreditinstituts kennt. Falls dieser noch nicht vorliegt, ist in beide Felder der Wert „999“ einzustellen.

Details siehe VI.5.1.1

Nr. 5: Zertifikat

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

Details siehe VI.5.1.4

- **Beispiel**

```
HKISA:8:2+2+124+280:10020030:12345:S:1:1'
```

VI.6.1.3 Übermittlung eines öffentlichen Schlüssels

♦ **Beschreibung**

Dieses Segment wird zum einen innerhalb der Dialoginitialisierungsantwort (vgl. Kapitel III.3.2) an den Kunden übertragen, falls sich der öffentliche Schlüssel des Kreditinstituts geändert hat. Es enthält dann jeweils einen öffentlichen Schlüssel des Kreditinstituts.

Zum anderen wird das Segment im Rahmen der erstmaligen Anforderung der öffentlichen Schlüssel des Kreditinstituts (vgl. Kapitel VI.6.2.2) benötigt.

♦ **Format**

Name: Übermittlung eines öffentlichen Schlüssels
Typ: Segment
Segmentart: Administration
Kennung: HIISA
Bezugssegment: HKISA
Segmentversion: 2
Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Nachrichtenbeziehung, kodiert	DE	num	1	M	1	1
3	Austauschkontrollreferenz	DE	id	#	M	1	
4	Nachrichtenreferenz-nummer	DE	num	..4	M	1	>0
5	Bezeichner für Funktions-typ	DE	num	..3	M	1	224
6	Schlüsselname	DEG			M	1	
7	Öffentlicher Schlüssel	DEG			M	1	
8	Zertifikat	DEG			K	1	

♦ **Erläuterungen**

Nr. 2: Nachrichtenbeziehung, kodiert

Es ist folgender Wert vorgesehen:

- "1" für ‘Key-Management-Nachricht ist Antwort’

Nr. 3: Austauschkontrollreferenz

Dialog-ID der Anfragenachricht des Kunden (vgl. Kapitel II.6.2).

Nr. 4: Nachrichtenreferenznummer

Nachrichtennummer der Anfragenachricht des Kunden (vgl. Kapitel II.6.2).

Nr. 5: Bezeichner für Funktionstyp

Es ist folgender Wert vorgesehen:

- "224" für ‘Certificate Status Notice’

Nr. 6: Schlüsselname

Der zurückgemeldete Schlüsselname enthält insbesondere die zugehörige Schlüssel- und Versionsnummer, die das Kundenprodukt für die Referenzierung des in der DEG „Öffentlicher Schlüssel“ übertragenen neuen öffentlichen Schlüssels verwendet.

Details siehe VI.5.1.1

Nr. 7: Öffentlicher Schlüssel

Diese Datenelementgruppe enthält den neuen öffentlichen Schlüssel des Kreditinstitutes.

Details siehe VI.5.1.5

Nr. 8: Zertifikat

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

Details siehe VI.5.1.4

♦ **Beispiel**

```
HIISA:8:2:8+1+4711+1+224+280:10020030:12345:S:1:
1+6:16:10:@12@<Modulus>:12:@3@<Exponent>:13'
```

VI.6.1.4 Schlüsselsperrung

♦ **Beschreibung**

Dieses Segment enthält die Anforderung für das Sperren eines Schlüssels.

♦ **Format**

Name: Schlüsselsperrung
Typ: Segment
Segmentart: Administration
Kennung: HKSSP
Bezugssegment: -
Segmentversion: 2
Sender: Kunde

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Nachrichtenbeziehung, kodiert	DE	num	1	M	1	2
3	Bezeichner für Funktionstyp	DE	num	..3	M	1	130
4	Schlüsselname	DEG			M	1	
5	Sperrenkennzeichen	DE	an	..3	M	1	1, 501, 999
6	Sicherheitsdatum und -uhrzeit	DEG			K	1	
7	Zertifikat	DEG			K	1	

♦ **Erläuterungen**

Nr. 2: Nachrichtenbeziehung, kodiert

Im Zusammenhang mit der Schlüsselsperrung ist folgender Wert vorgesehen:

- "2" für 'Key-Management-Nachricht erwartet Antwort'

Nr. 3: Bezeichner für Funktionstyp

Im Zusammenhang mit der Schlüsselsperrung ist folgender Wert vorgesehen:

- "130" für 'Certificate Revocation' (Zertifikatswiderruf)

Nr. 4: Schlüsselname

Es sind die Identifikationsmerkmale des zu sperrenden Signierschlüssels einzustellen, unabhängig davon, daß grundsätzlich immer sowohl Signier- als auch Chiffrierschlüssel gesperrt werden (s. Kap. VI.6.2.4).

Format siehe VI.5.1.1

Nr. 5: Sperrenkennzeichen

Enthält folgende Werte als Begründung für die Sperrung:

- "1" für 'Schlüssel des Zertifikatseigentümers kompromittiert'

- "501" für ‘Zertifikat ungültig wegen Verdacht auf Kompromittierung’
- "999" für ‘gesperrt aus sonstigen Gründen’

Nr. 6: Sicherheitsdatum und -uhrzeit

Enthält optional Datum und Uhrzeit, ab welcher der Schlüssel nicht mehr gültig ist. Als Bedeutung wird „6“ eingestellt, da Datum und Zeit das Ende der Gültigkeit anzeigen.

Details siehe VI.5.1.2

Es ist zu beachten, daß eine terminierte Sperre nicht von allen Kreditinstituten unterstützt wird. Das Kundenprodukt sollte den Kunden auf diesen Sachverhalt hinweisen.

Nr. 7: Zertifikat

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

Details siehe VI.5.1.4

♦ **Beispiel**

```
HKSSP:8:2+2+130+280:10020030:12345:S:1:1+501'
```

VI.6.1.5 Bestätigung der Schlüsselsperrung

♦ **Beschreibung**

Dieses Segment enthält die Bestätigung für eine Schlüsselsperrung.

♦ **Format**

Name: Bestätigung der Schlüsselsperrung
Typ: Segment
Segmentart: Administration
Kennung: HISSP
Bezugssegment: HKSSP
Segmentversion: 2
Sender: Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Nachrichtenbeziehung, kodiert	DE	num	1	M	1	1
3	Austauschkontrollreferenz	DE	id	#	M	1	
4	Nachrichtenreferenz-nummer	DE	num	..4	M	1	>0
5	Bezeichner für Funktions-typ	DE	num	..3	M	1	231
6	Schlüsselname	DEG			M	1	
7	Sperrenkennzeichen	DE	an	..3	M	1	1, 501, 999
8	Sicherheitsdatum und -uhrzeit	DEG			M	1	
9	Zertifikat	DEG			K	1	

♦ **Erläuterungen**

Nr. 2: Nachrichtenbeziehung, kodiert

Im Zusammenhang mit der Schlüsselsperrung ist folgender Wert vorgesehen:

- "1" für ‘Key-Management-Nachricht ist Antwort’

Nr. 3: Austauschkontrollreferenz

Dialog-ID der Sperrnachricht des Kunden (vgl. Kapitel II.6.2).

Nr. 4: Nachrichtenreferenznummer

Nachrichtennummer der Sperrenanforderung des Kunden (vgl. Kapitel II.6.2).

Nr. 5: Bezeichner für Funktionstyp

Im Zusammenhang mit der Schlüsselsperrung ist folgender Wert vorgesehen:

- "231" für ‘Revocation Confirmation’ (Bestätigung des Zertifikatswiderrufs)

Nr. 6: Schlüsselname

Es sind die Identifikationsmerkmale des gesperrten Signierschlüssels einzustellen, unabhängig davon, daß grundsätzlich immer sowohl Signier- als auch Chiffrierschlüssel gesperrt werden (s. Kap. VI.6.2.4).

Format siehe VI.5.1.1

Nr. 7: Sperrenkennzeichen

Kann folgende Werte enthalten:

- "1" für ‘Schlüssel des Zertifikatseigentümers kompromittiert’
- "501" für ‘Zertifikat ungültig wegen Verdacht auf Kompromittierung’
- "999" für ‘gesperrt aus sonstigen Gründen’

Nr. 8: Sicherheitsdatum und -uhrzeit

Enthält Datum und Uhrzeit, ab welchem das Zertifikat nicht mehr gültig sein soll. Als Bedeutung wird „6“ eingestellt, da Datum und Zeit das Ende der Gültigkeit anzeigen.

Details siehe VI.5.1.2

Nr. 9: Zertifikat

Hier wird bei späterem Einsatz von Zertifizierungsinstanzen vom Kreditinstitut ein Zertifikat transparent eingestellt, um die Sperrung zu bestätigen.

Details siehe VI.5.1.4

♦ **Beispiel**

```
HISSP:8:2:8+1+4711+2+231+280:10020030:12345:S:1:
1+501+6:19960611:111734'
```

VI.6.2 Key-Management-Nachrichten

Aufträge des Key-Managements dürfen nur in den folgenden separaten Nachrichten übertragen werden.

Hiervon abweichend wird der Auftrag „Anforderung eines öffentlichen Schlüssels des Kreditinstituts“ nicht als eigene Nachricht, sondern innerhalb der Dialoginitialisierung übertragen.

Die Nachrichten für das Key-Management müssen zum Teil kryptographisch geschützt werden. Alternativ können auch Offline-Sicherungsverfahren (z.B. Brief) zum Einsatz kommen (vgl. Kapitel VI.3.1.3).

Es sind folgende Key-Management-Nachrichten vorgesehen:

- Änderung eines öffentlichen Schlüssels des Kunden
- Erstmalige Anforderung der Schlüssel des Kreditinstituts
- Erstmalige Übermittlung der Schlüssel des Kunden
- Schlüsselsperrung den Kunden

Mit Ausnahme der Sperrnachricht sind alle Key-Management-Nachrichten nur bei Einsatz des RDH-Verfahrens möglich.

VI.6.2.1 Änderung eines öffentlichen Schlüssels des Kunden

Realisierung Bank: verpflichtend
Realisierung Kunde: verpflichtend

a) Kundennachricht

♦ **Beschreibung**

Diese Nachricht ist nur bei Verwendung des RDH-Verfahrens möglich. Der Nachricht muß eine Dialoginitialisierung vorausgehen. Der Auftrag muß mit dem alten Signierschlüssel signiert werden.

Zum Verfahren s. Kap. VI.3.1.3.3.

♦ **Format**

Name: Änderung eines öffentlichen Schlüssels des Kunden
Typ: Nachricht
Sender: Kunde

Nr.	Name	Typ	Kennung	Status	Anzahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	M	1	s. Kap. VI.5.2
3	Schlüsseländerung	SEG	HKSAK	M	1-2	s. Kap. VI.6.1.1
4	Signaturabschluß	SEG	HNSHA	M	1	s. Kap. VI.5.3
5	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

♦ **Erläuterungen**

Nr. 3: Schlüsseländerung

Der Kunde stellt entweder seinen neuen öffentlichen Signierschlüssel, seinen neuen öffentlichen Chiffrierschlüssel oder beide Schlüssel ein.

b) Kreditinstitutsnachricht

♦ **Format**

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

♦ **Erläuterungen**

Es werden keine Datensegmente zurückgemeldet.

♦ **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel
0020	Öffentlicher Schlüssel wurde geändert
9010	Schlüsseländerung zur Zeit nicht möglich
9010	Sicherheitsverfahren unterstützt keine öffentlichen Schlüssel
9210	Eingereichter Schlüssel ist mit dem aktuellen Schlüssel identisch

VI.6.2.2 Erstmalige Anforderung der Schlüssel des Kreditinstituts

Mit Hilfe dieser Nachricht fordert der Kunde erstmalig den öffentlichen Signier- und Chiffrierschlüssel des Kreditinstituts an. Gleichzeitig erhält er die aktuellen Bankparameterdaten, die er benötigt, um die unterstützten Verschlüsselungsverfahren des Kreditinstituts in Erfahrung zu bringen. Mit Hilfe dieser Informationen wird der Kunde in die Lage versetzt, beliebige Nachrichten zu verschlüsseln.

Realisierung Bank: optional
Realisierung Kunde: verpflichtend

a) Kundennachricht

♦ **Beschreibung**

Diese Nachricht wird an Stelle einer Dialoginitialisierung gesendet. Es dürfen keine Auftragsnachrichten folgen. Der Dialog ist vom Kunden nach Erhalt der Antwortnachricht mit einer Dialogendenachricht zu beendigen. Die Nachricht wird weder signiert noch verschlüsselt.

♦ **Format**

Name: Erstmalige Anforderung der Schlüssel des Kreditinstituts
Typ: Nachricht
Sender: Kunde

Nr.	Name	Typ	Kennung	Status	Anzahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Identifikation	SEG	HKIDN	M	1	s. Kap. III.3.1.2
3	Verarbeitungsvorbereitung	SEG	HKVVB	M	1	s. Kap. III.3.1.3
4	Anforderung eines öffentlichen Schlüssels	SEG	HKISA	M	2	s. Kap. VI.6.1.2
5	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

♦ **Erläuterungen**

Nr. 2: Identifikation

Die Datenelemente des Segments sind wie beim anonymen Zugang zu belegen (s. Kap. III.5).

Nr. 3: Verarbeitungsvorbereitung

Mit diesem Segment fordert der Kunde die Bankparameterdaten an.

Nr. 4: Anforderung eines öffentlichen Schlüssels

Mit diesen beiden Segmenten fordert der Kunde jeweils den öffentlichen Signierschlüssel und den öffentlichen Chiffrierschlüssel des Kreditinstituts an. Es sind stets beide Schlüssel anzufordern, auch wenn das Kreditinstitut nicht signiert.

b) Kreditinstitutsnachricht

♦ **Format**

Name: Erstmalige Übermittlung der Schlüssel des Kreditinstituts
Typ: Nachricht
Sender: Kreditinstitut

Nr.	Name	Typ	Kennung	Status	Anzahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	K	0-1	s. Kap. VI.5.2
3	Rückmeldungen zur Gesamtnachricht	SEG	HIRMG	M	1	s. Kap. II.8.2
4	Rückmeldungen zu Segmenten	SEG	HIRMS	K	0-n	s. Kap. II.8.3
5	Bankparameterdaten	SF	#	K	1	s. Kap. III.3.2.2
6	Übermittlung eines öffentlichen Schlüssels	SEG	HIISA	M	1-2	s. Kap. VI.6.1.3
7	Signaturabschluß	SEG	HNSHA	K	0-1	s. Kap. VI.5.3
8	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

♦ **Erläuterungen**

Nr. 2: Signaturkopf

Falls das Kreditinstitut einen Signierschlüssel besitzt, d.h. seine Nachrichten grundsätzlich signiert, hat es auch diese Nachricht zu signieren, um die Authentizität des Chiffrierschlüssels zu sichern (s.u.).

Nr. 6: Übermittlung eines öffentlichen Schlüssels

In diesen beiden Segmenten werden dem Kunden die öffentlichen Schlüssel des Kreditinstituts mitgeteilt.

Falls das Kreditinstitut seine Nachrichten nicht signiert, erhält der Kunde nur den öffentlichen Chiffrierschlüssel zurückgemeldet. Auf die Anforderung des Signierschlüssels erhält er einen entsprechenden Rückmeldungscode, der ihm anzeigt, daß das Kreditinstitut seine Nachrichten nicht signiert. Da die Authentizität des Chiffrierschlüssels nicht gesichert ist, muß diese Nachricht durch einen Ini-Brief an den Kunden mit dem Hashwert des Chiffrierschlüssels begleitet werden (s. Kap. VI.3.1.3.2).

Falls das Kreditinstitut seine Nachrichten signiert, erhält der Kunde sowohl den öffentlichen Chiffrier- als auch Signierschlüssel zurückgemeldet. Die Authentizität des Chiffrierschlüssels ist dabei durch die Signatur gesichert. Die Authentizität des Signierschlüssels ist jedoch nicht gesichert, da das Kundensystem die Echtheit der Signatur nicht prüfen kann. Daher muß in diesem Fall die Nachricht durch einen Ini-Brief mit dem Hashwert des Signierschlüssels begleitet werden.

♦ **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel
0020	Auftrag ausgeführt
9010	Kein Schlüssel verfügbar, da Kreditinstitutsnachrichten nicht signiert werden

VI.6.2.3 Erstmalige Übermittlung der Schlüssel des Kunden

Mit Hilfe dieser Nachricht übermittelt der Kunde erstmalig seinen öffentlichen Signier- und Chiffrierschlüssel an das Kreditinstitut („Erstinitialisierungsnachricht“).

Da der Absender des öffentlichen Schlüssels den Beweis erbringen muß, daß er auch im Besitz des zugehörigen privaten Schlüssels ist, muß die Nachricht des Kunden signiert sein.

Das Kreditinstitut darf eine Nachricht nicht ablehnen, nur weil für den Kunden noch kein öffentlicher Schlüssel in der Schlüsselverwaltung existiert. Falls die normale Signaturprüfung aus diesem Grund negativ verläuft, muß zunächst geprüft werden, ob es sich um eine Erstinitialisierung handelt. In diesem Fall ist der öffentliche Schlüssel aus der Erstinitialisierungsnachricht zu extrahieren und die Signaturprüfung auf der Basis dieses Schlüssels erneut vorzunehmen.

Die Erstinitialisierungsnachricht des Kunden ist zu verschlüsseln, da die darin enthaltenen benutzerbezogenen Daten (Kunden-ID, Benutzerkennung) als vertraulich einzustufen sind. Dies erfordert, daß sich der öffentliche Chiffrierschlüssel des Kreditinstituts schon vor dem Senden der Erstinitialisierung im Besitz des Kunden befinden muß. Ferner muß dem Kunden das Verschlüsselungsverfahren bekannt sein, das ihm in den Bankparameterdaten mitgeteilt wird. Um dem Kunden diese Daten vorab zukommen zu lassen bieten sich folgende Lösungen an:

- Das Kreditinstitut sendet dem Kunden eine Diskette zu, die die Schlüssel und die aktuelle BPD enthält, wie in VI.3.1.3.2 beschrieben.
- Der Kunde sendet die Key-Management-Nachricht „Erstmalige Anforderung der Schlüssel des Kreditinstituts“ (s. Kap. VI.6.2.2). Diese Nachricht wird begleitet von einem Ini-Brief.

Um die wiederholte Ausführung unberechtigter Initialisierungsversuche zu verhindern, sind kreditinstitutsseitig folgende Vorkehrungen zu treffen:

- Die Benutzerkennung sollte bei Verwendung des RDH-Verfahrens nicht durch benutzerindividuelle Merkmale (z.B. Kontonummer) hergeleitet werden können.
- Eine weitere Erstinitialisierung unter derselben Benutzerkennung und Kunden-ID hat zur Ablehnung der Nachricht zu führen.

Realisierung Bank: verpflichtend
Realisierung Kunde: verpflichtend

a) Kundennachricht

♦ Beschreibung

Diese Nachricht wird an Stelle einer Dialoginitialisierung gesendet. Es dürfen keine Auftragsnachrichten folgen. Der Dialog ist vom Kunden nach Erhalt der Antwortnachricht mit einer Dialogendenachricht zu beendigen. Die Nachricht muß signiert und verschlüsselt werden.

♦ Format

Name: Erstmalige Übermittlung der Schlüssel des Kunden
Typ: Nachricht
Sender: Kunde

Nr.	Name	Typ	Kennung	Status	Anzahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	M	1	s. Kap. VI.5.2
3	Identifikation	SEG	HKIDN	M	1	s. Kap. III.3.1.2
4	Schlüsseländerung	SEG	HKSAK	M	2	s. Kap. VI.6.1.1
5	Signaturabschluß	SEG	HNSHA	M	1	s. Kap. VI.5.3
6	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

♦ Erläuterungen

Nr. 3: Identifikation

Der Benutzer hat die ihm zur Initialisierung mitgeteilten Daten einzustellen. Da zu diesem Zeitpunkt noch keine Synchronisierung durchgeführt wurde, ist als Kundensystem-ID der Wert ‘0’ einzustellen.

Nr. 4: Schlüsseländerung

Der Kunde stellt seinen öffentlichen Signier- und Chiffrierschlüssel ein.

Die Authentizität des Chiffrierschlüssels ist dabei durch die Signatur gesichert. Die Authentizität des Signierschlüssels ist jedoch nicht gesichert, da das Kreditinstitut die Echtheit der Signatur nicht prüfen kann. Daher muß die Nachricht durch einen Ini-Brief an das Kreditinstitut mit dem Hashwert des Signierschlüssels begleitet werden (s. Kap. VI.3.1.3.2).

b) Kreditinstitutsnachricht

♦ **Beschreibung**

Die Ablehnung der Erstinitialisierungsnachricht darf aus sicherheitstechnischen Aspekten im Rahmen der Rückmeldungscodes nicht inhaltlich begründet werden. Fehlermeldungen, die sich auf den syntaktischen Aufbau der Nachricht bzw. der Segmente beziehen, sind hiervon unberührt.

♦ **Format**

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

♦ **Erläuterungen**

Es werden keine Datensegmente zurückgemeldet.

♦ **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel
0010	Öffentlicher Schlüssel wurde entgegengenommen
0020	Öffentlicher Schlüssel wurde freigeschaltet
0020	Kunde wurde freigeschaltet
9010	Auftrag abgelehnt

VI.6.2.4 Schlüsselsperrung durch den Kunden

Diese Nachricht beschreibt die Anforderung zum Sperren der Schlüssels durch den Kunden und die Bestätigung der Schlüsselsperrung durch das Kreditinstitut (vgl. Kapitel VI.3.3).

Realisierung Bank: verpflichtend
Realisierung Kunde: verpflichtend

a) Kundennachricht

♦ **Beschreibung**

Es werden immer beide Schlüssel (Signier- und Chiffrierschlüssel) gesperrt. Eine selektive Schlüsselsperrung ist gegenwärtig nicht zulässig.

Der Nachricht muß eine Dialoginitialisierung vorausgehen. Die Nachricht muß bei Kompromittierung signiert sein. Es liegt in der Entscheidung des Kreditinstituts, ob es auch nicht signierte (anonyme) Schlüsselsperrungen erlaubt (z.B. bei Verlust des Sicherheitsmediums). Die Steuerung erfolgt in den Userparameterdaten über das Feld „Anzahl benötigter Signaturen“.

Bei Verlust des Sicherheitsmediums liegen dem Benutzer u.U. die zur Durchführung der Sperrung erforderlichen Daten (Schlüsselnummer und -version) nicht vor. In diesem Fall ist zur Referenzierung auf den aktuellen Schlüssel jeweils der Wert ‘999’ einzustellen. Es ist daher darauf zu achten, daß dieser Wert reserviert ist und nicht im Rahmen der Versionszählung belegt wird.

Falls das Kreditinstitut unsignierte Sperrungen zuläßt, muß dem Benutzer darüber hinaus explizit seine Benutzerkennung mitgeteilt werden. Beim RDH-Verfahren erfolgt dies im Rahmen des Ini-Briefs. Beim DDV-Verfahren kann diese dem Benutzer bei der Aushändigung der Chipkarte mitgeteilt werden.

Beim RDH-Verfahren muß der Kunde nach einer Schlüsselsperrung zur Entsperrung eine erneute Erstinitialisierung durchführen.

♦ **Format**

Name: Sperrung eines Schlüssels durch den Kunden
Typ: Nachricht
Sender: Kunde

Nr.	Name	Typ	Kennung	Status	Anzahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	K	0-1	s. Kap. VI.5.2
3	Schlüsselsperrung	SEG	HKSSP	M	1	s. Kap. VI.6.1.4
4	Signaturabschluß	SEG	HNSHA	K	0-1	s. Kap. VI.5.3
5	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

♦ **Erläuterungen**

Nr. 3: Schlüsselsperrung

Dieses Segment enthält die Anforderung für die Schlüsselsperrung.

Eine selektive Schlüsselsperrung ist gegenwärtig nicht zulässig, d.h. es werden immer beide Schlüssel (Signier- und Chiffrierschlüssel) gleichzeitig gesperrt. In der DEG „Schlüsselname“ sind die Merkmale des Signierschlüssels einzustellen (s. Kap. VI.6.1.4).

b) Kreditinstitutsnachricht

♦ **Format**

Name: Bestätigung der Schlüsselsperrung durch das Kreditinstitut
Typ: Nachricht
Sender: Kreditinstitut

Nr.	Name	Typ	Kennung	Status	Anzahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. Kap. II.6.2
2	Signaturkopf	SEG	HNSHK	K	0-1	s. Kap. VI.5.2
3	Rückmeldungen zur Gesamtnachricht	SEG	HIRMG	M	1	s. Kap. II.8.2
4	Rückmeldungen zu Segmenten	SEG	HIRMS	K	0-n	s. Kap. II.8.3
5	Bestätigung der Schlüsselsperrung	SEG	HISSP	M	1	s. Kap. VI.6.1.5
6	Signaturabschluß	SEG	HNSHA	K	0-1	s. Kap. VI.5.3
7	Nachrichtenabschluß	SEG	HNHBS	M	1	s. Kap. II.6.3

♦ **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel
0020	Schlüssel wurde erfolgreich gesperrt
9010	Schlüssel ist bereits gesperrt
9010	Terminierte Sperren werden nicht unterstützt
9210	Unbekanntes Sperrenkennzeichen
9210	Sperrdatum liegt zu weit in der Zukunft