HBCI – Eine sichere Plattform *nicht nur* für Homebanking

René Algesheimer Detlef Hühnlein

secunet Security Networks GmbH

Mergenthalerallee 79-81

D-65760 Eschborn

algesheimer@secunet.de huehnlein@secunet.de

Zusammenfassung

Die im Zentralen Kredit Ausschuß (ZKA) organisierten deutschen Banken haben sich im Homebanking-Abkommen zum 01.10.1998 auf die breite Einführung des neuen Home Banking Computer Interfaces (HBCI) für die Abwicklung von Online-Bank-Transaktionen geeinigt. In diesem Beitrag wollen wir die wichtigsten Merkmale von HBCI kurz vorstellen. Insbesondere zeigt die Erörterung von HBCI, daß die bald flächendeckend vorhandene HBCI-Infrastruktur auch sehr gut für nicht-bankenspezifische ‚X-HBCI'-Transaktionen genutzt werden kann. In diesem Beitrag wollen wir abstrakte Merkmale für Anwendungsszenarien, in denen die Verwendung von HBCI sinnvoll erscheint, herleiten und für konkrete Beispiele, wie Behörden-Transaktionen, neue ‚X-HBCI'-Geschäftsvorfälle definieren.

1 Einleitung

Die Anzahl der Online-Konten in Deutschland erfährt ein stetiges Wachstum. Der Löwenanteil der deutschen Banken bietet seinen Kunden die Möglichkeit der Kontoführung über z.B. T-Online oder dem Internet an. Vor der Verabschiedung von HBCI 1.0 im Jahre 1996 existierten bereits Homebanking-Lösungen verschiedener Banken auf Basis des „ZKA-Dialogs", einer 1987 von den deutschen Banken standardisierten BTX/CEPT – Ausprägung, oder andere proprietären Verfahren auf z.B. SSL-Basis. Neben der offensichtlich ***umständlichen Handhabung der PIN/TANs*** für den Kunden gab es noch eine Reihe weiterer schwerwiegender Probleme:

- Der ZKA-Dialog war ***nur für BTX/CEPT/T-Online*** konzipiert; andere Transport- und Präsentationsdienste wurden nicht direkt unterstützt.
- In unsicheren offenen Netzen sind ***zusätzliche Sicherheitsmechanismen nötig***.
- Da der ZKA-Dialog nur halbherzig standardisiert wurde, entwickelten sich verschiedene, wechselseitig inkompatible, „Dialekte". Von ***„Multibank-Fähigkeit"***, d.h. Verwaltung mehrerer Konten bei verschiedenen Kreditinstituten, war also keine Rede.
- Die ***Betriebssicherheit*** ließ zu wünschen übrig. Brach während einer Sitzung die Leitung ab, so konnte nicht direkt, d.h. ohne Überprüfung des Konto-Auszuges, geklärt werden, ob die letzte Transaktion angenommen wurde.

Deshalb kam man nicht umhin einen neuen Standard für Homebanking festzulegen, der die oben angerissenen Probleme lösen soll. Das Ergebnis war HBCI, was wir in Kapitel 0 näher erörtern wollen. Man wird sehen, daß viele der Design-Ziele HBCI's keineswegs bank-spezifisch sind, sondern vielmehr eine einheitliche, flexible, erweiterbare Sicherheitsplattform für formatierte Transaktionen jeglicher Art beschreiben. Deshalb ist es naheliegend, HBCI und die bald flächendeckend verfügbare HBCI-Infrastruktur zu nutzen, um auch andere Online-Transaktionen in sicherer Art und Weise durchzuführen. Diese Idee wird in Kapitel 0 aufgegriffen, wo wir abstrakte Merkmale potentieller Einsatzgebiete für dieses „X-HBCI" angeben und in Kapitel 4 anhand eines konkreten Beispieles zeigen, wie neue Geschäftsvorfälle aussehen könnten. In Kapitel 0 wollen wir den Beitrag mit einem Blick auf die Zukunft von (X-)HBCI abschließen.

2 HBCI – Der neue Homebanking-Standard

In diesem Kapitel wollen wir ganz kurz die wichtigsten Merkmale des neuen, von allen deutschen Banken unterstützten, Homebanking-Standards HBCI anführen. Für eine ausführlichere Darstellung verweisen wir auf [HBCIKOMP] oder [HBCISPEC].

Will ein Kunde Bankgeschäfte mittels einer Online-Verbindung tätigen, so initiiert er eine logische Verbindung zu seiner Bank. Diese ***Dialog-Initialisierung*** dient der Authentisierung

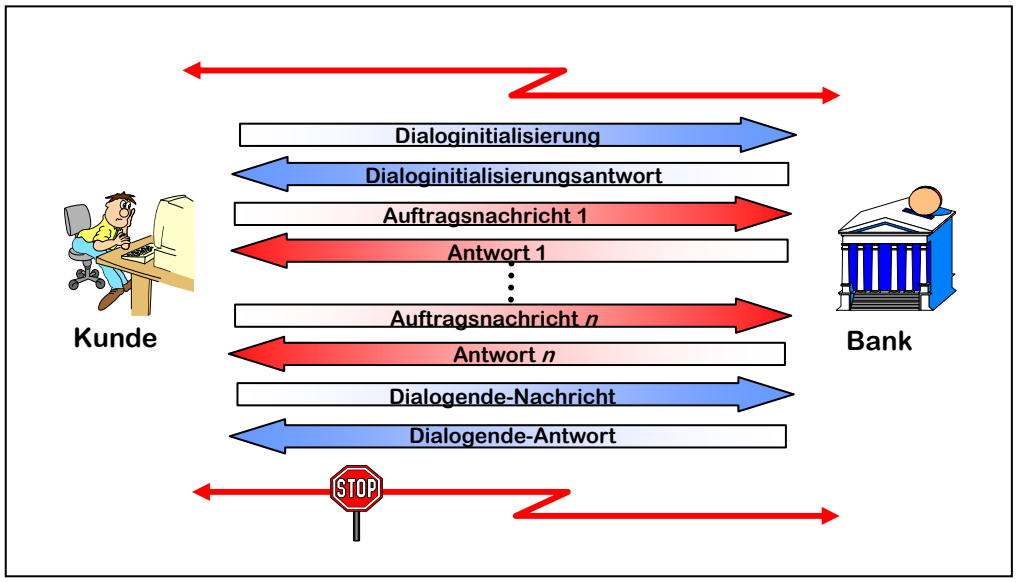

Abbildung 1: Dialogablauf

der beiden Parteien und der Synchronisation der fortlaufenden Nachrichten-Nummer. Somit kann festgestellt werden, ob die letzte gesendete Transaktions-Nachricht vom Kreditinstitut erfolgreich verarbeitet werden konnte. Zusätzlich werden bei der Dialog-Initialisierung auch die Verschlüsselungs- und Kompressionsverfahren ausgehandelt und ggf. User-Parameterdaten (UPD) und Bank-Parameterdaten (BPD) abgeglichen. Nach erfolgreicher Dialoginitialisierung, wie in Abbildung 1 dargestellt, schickt der Kunde ***Auftragsnachrichten*** an die Bank, die einzeln von der Bank quittiert werden. Es ist möglich, daß die gesamte Verarbeitung der Aufträge ***synchron*** erfolgt, d.h. der Kunde hält die Verbindung und wartet bis das Kreditinstitut den jeweiligen Auftrag abgearbeitet hat. Daneben ist es möglich die Verarbeitung der Aufträge ***asynchron*** durchzuführen. Dabei signalisiert die Bank in der jeweiligen Antwortnachricht lediglich, daß der Auftrag eingegangen ist. Der Kunde kann nach der Übermittlung der Aufträge die Verbindung beenden und bei einer späteren Sitzung

ein Statusprotokoll anfordern um sich über den aktuellen Stand der Verarbeitung zu informieren.

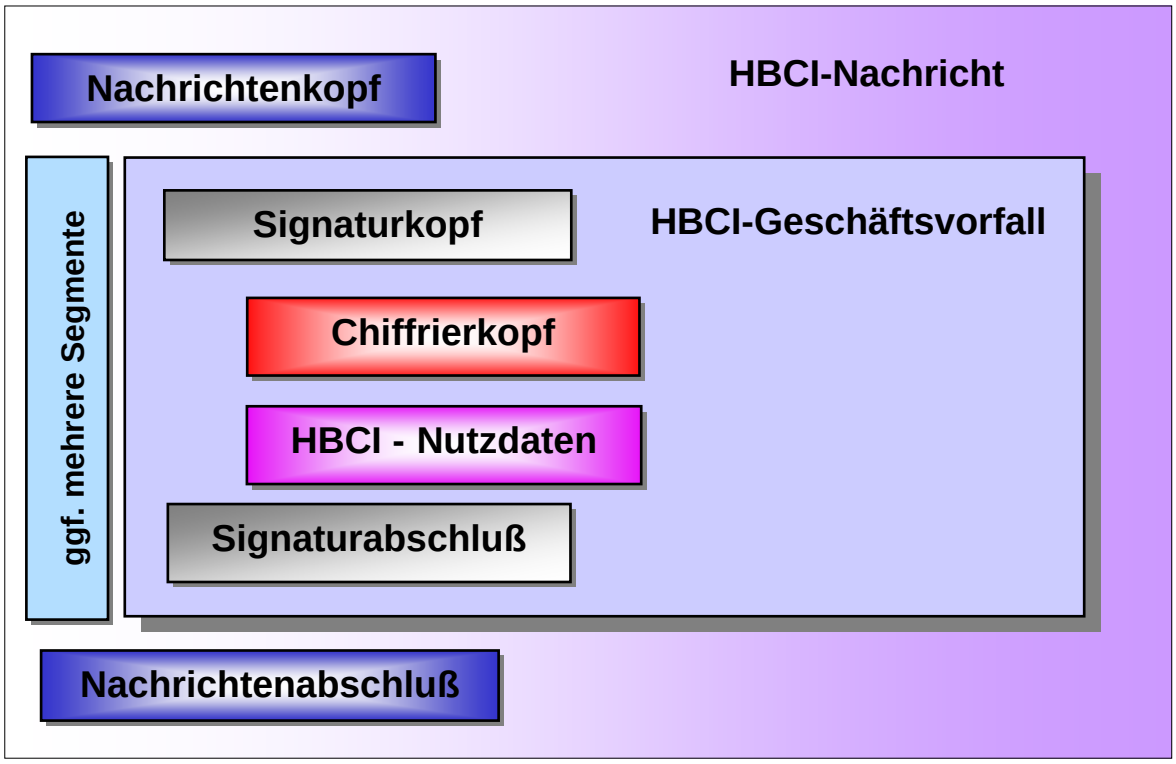

Abbildung 2: Nachrichtenaufbau

Der Aufbau einer Auftrags- oder Antwort-Nachricht ist schematisch in Abbildung 2 dargestellt; ein konkretes Beispiel einer HBCI-Nachricht findet sich im Anhang. HBCI ist eine sog. ***Nettodaten-Schnittstelle*** mit ***Trennzeichen-Syntax***. Das bedeutet, daß die übertragenen Daten, im Gegensatz zu einer z.B. ASN.1-Codierung, keine Information über Ihre Struktur enthalten. Das hat den Vorteil, daß keine Bandbreite durch Struktur-Informationen „verschwendet“ wird. Allerdings muß die Struktur einer z.B. Überweisung bei beiden Kommunikationspartnern bekannt sein. Neben ***HBCI-spezifischen Formaten***, können auch Binärdaten transparent eingestellt werden. Somit können ***Daten jeglicher Art*** mit HBCI auf sicherer Art und Weise transportiert werden.

In Abbildung 2 ist auch ersichtlich, daß die Verwendung gewisser Sicherheitsmechanismen, wie Verschlüsselung und Signatur vorgesehen ist. In der derzeitigen Spezifikation 2.01 sind für die Verschlüsselung zwei verschiedene Verfahren vorgesehen: Entweder das DES-DES-Verfahren (DDV), d.h. 2-Key-Triple-DES mit Chipkarte, oder das RSA-DES-Hybrid-Verfahren (RDH) als Software-Lösung oder mit Chipkarte. Verschlüsselt wird lediglich ein 2-Key-Triple-DES-Session-Key. Für die Berechnung der Signatur wird entweder 768-Bit-RSA oder ein Triple-DES-MAC verwendet. In beiden Fällen wird RIPEMD-160 für die Berechnung des Hash-Wertes verwendet. Die beiden heute meist verwendeten Ausprägungen (DDH mit Chipkarte oder RDH in Software) dürfen lediglich als Migrationswege angesehen werden:

> „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.“ (siehe [HBCISPEC] – Teil B, Seite 2).

Diese „technischen Restriktionen“ bestehen zum Großteil in der Verfügbarkeit kostengünstiger Chipkarten, die in der Lage sind digitale Signaturen mit z.B. RSA zu berechnen. Deshalb sollte die HBCI-Spezifikation um Sicherungsmechanismen auf Basis Elliptischen Kurven erweitert werden, da hier (siehe z.B. [HÜ98]) eine Implementierung auf kostengünstigen Chipkarten ***ohne Koprozessor*** möglich ist.
Wie wir sahen, ähnelt HBCI im Sicherheitsbereich stark Schnittstellen-Definitionen, wie EDIFACT. Insgesamt ist HBCI derart konzipiert, daß es flexibel um neue Geschäftsvorfälle, Sicherheitsmechanismen, sowie Übertragungs- und Präsentationsmedien erweitert werden kann. Der Grad der Sicherheit und der Aufwand für eine solche Transaktion gründet in den jeweils verwendeten Sicherheitsverfahren.

Diese Möglichkeiten machen HBCI zu einer derzeit konkurrenzlosen Plattform für Online-Transaktionen. Da sich alle deutschen Banken zur Unterstützung von HBCI verpflichtet haben, besteht die Möglichkeit mit ein und dem selben Homebanking-Client Konten bei verschiedensten Kreditinstituten zu verwalten. Insgesamt darf also damit gerechnet werden, daß mittelfristig die HBCI-Infrastruktur beim Online-Kunden vorhanden ist. Da bei der Konzeption von HBCI tunlichst auf Flexibilität und Erweiterbarkeit geachtet wurde, liegt es nahe die bald vorhandene Kunden-Infrastruktur für andere, ***nicht-bankspezifische, Online-Transaktionen*** zu verwenden. Diese Idee wollen wir im nächsten Abschnitt etwas konkretisieren.

3 ... - auch außerhalb der Bankenwelt

In diesem Kapitel wollen wir abstrakte Merkmale möglicher Anwendungsszenarien ableiten, für die die Verwendung von HBCI als Sicherheitsplattform sinnvoll erscheint. Danach wollen wir anhand konkreter Beispiele aufzeigen, wie neue Geschäftsvorfälle für diese Szenarien aussehen könnten. Diese Möglichkeiten für sogenannte X-HBCI Vorfälle müssen jedoch zunächst vom ZKA akzeptiert und standardisiert werden, bevor sie in Kraft treten können.

Mögliche Anwendungsszenarien für HBCI außerhalb des Bankenumfeldes sollten folgende Merkmale haben:

- Die Transaktionen werden ***vom Kunden angestoßen***.
- Die Transaktionen sollten ***mehrmals wiederkehrend*** vorkommen, wobei der Zeitpunkt der Transaktion nicht absehbar ist.
- Die Transaktion sollte ***formulargebunden***, d.h. nicht völlig formlos, ablaufen.
- Die angeforderte Dienstleistung bzw. das Gut sollte ***elektronisch übermittelbar*** sein. Im Idealfall sollte das übermittelte Gut wiederum einem gewissen vorher festgelegtem ***Format*** genügen.
- Die Transaktion sollte ***quittiert*** werden müssen.
- Besonders vorteilhaft ist die Verwendung von HBCI, wenn die Transaktion ***mit einer Bezahlung gekoppelt*** ist. Der Betrag einer solchen Transaktion sollte nicht allzu klein sein, damit sich eine Überweisung überhaupt lohnt.

Es ist leicht, zu diesen abstrakten Merkmalen, teilweise visionäre, Anwendungsszenarien zu finden, für die HBCI eine geeignete Plattform darstellt. Wir führen einige Beispiele an:

- ***Elektronische Reise-Tickets***
  Ein Verkehrsunternehmen, wie z.B. die Deutsche Bahn AG, bietet als Kunden-Service die Reisebuchung per Internet an. Diese Reisebuchung könnte nun per HBCI durchgeführt werden, wobei die Buchungsdaten in Form eines HBCI-Geschäftsvorfalles zur Bahn übertragen werden. Gleichzeitig schickt der Kunde eine signierte Überweisung über den entsprechenden Betrag. Im Gegenzug verschickt die Bahn das Ticket, beim heutigen Stand der Technik mit der Post. Ist die nächste Generation der Bahn-Card mit einem Chip ausgestattet, so kann das elektronische Ticket per HBCI übertragen und auf der Bahn-Card gespeichert werden. Somit stehen die bei der Fahrscheinkontrolle ermittelten Daten sofort für dem internen Controlling der Bahn zur Verfügung. Sind noch nicht bei allen Schaffnern entsprechende Lesegeräte vorhanden, um das elektronische Ticket auf der Karte zu überprüfen, so könnte sich der Kunde sein bereits gekauftes Ticket, wie z.B. bei der Lufthansa, an einem „E-TIX“ Automaten ausdrucken lassen. Wie die entsprechenden HBCI-Geschäftsvorfälle konkret aussehen könnten, werden wir später erörtern.
- ***Elektronische Veranstaltungs-Tickets***
  Das oben für Reise-Tickets erläuterte gilt im wesentlichen auch für Veranstaltungs-Tickets, wie Kino- oder Theater-Karten, Eintrittskarten für Sportveranstaltungen etc.
- ***Elektronische Briefmarken***
  Während heute übliche Frankiermaschinen meist bei der Post aufgeladen werden müssen, so könnte die Post auch, entsprechend kryptographisch behandelte, von gewöhnlichen PC’s erzeugte, Briefmarken zulassen. Der Ladevorgang für den PC als virtuelle Frankiermaschine könnte leicht über HBCI abgewickelt werden. Die Anzahl und der Einzelwert der Marken würde, zusammen mit einer entsprechenden Überweisung zur Post gesandt. Im Gegenzug erhält der Kunde über HBCI die kryptographisch gesicherten elektronischen Briefmarken von der Post.
- ***Elektronische Behördengänge***
  Nicht alle Besuche in Ämtern müssen physikalisch geschehen. Als ein Beispiel sei das Einwohner-Meldeamt genannt. Nach einem Umzug könnte die Ummeldung auch online erfolgen. Man würde einen HBCI-Dialog mit seiner Stadt- oder Gemeindeverwaltung aufbauen, und die neue Adresse innerhalb eines HBCI-Geschäftsvorfalles übermitteln. Fallen für die Ummeldung Gebühren an, so schickt man eine entsprechende Überweisung mit.
- ***HBCI-Studentenausweis***
  Auch im universitären Umfeld ist die Abwicklung von Verwaltungsaufgaben mit HBCI denkbar. So wären Geschäftsvorfälle wie die Immatrikulation, Rückmeldung, Prüfungsanmeldung, Abfrage von Prüfungsergebnissen und z.B. die Bestellung von Büchern in der Bibliothek denkbar. Die Semestergebühren könnten mit einer Überweisung die zusammen mit der Immatrikulation bzw. Rückmeldung verschickt wird bezahlt werden.
- ***Internet-Shopping***
  Werden z.B. im Internet Güter oder Dienstleistungen bestellt, so könnte die Zahlung dieser durch HBCI-Überweisungen geschehen. Bei größeren Bestellungen könnten EDIFACT-Datensätze transparent in HBCI-Geschäftsvorfälle eingestellt werden. Damit könnten die Bestellungen sofort den entsprechend nachgelagerten z.B. Logistik-, Dispositions- und Buchhaltungssystemen zugeführt werden. Werden digitale Waren, wie z.B. ein Artikel bei einer Online-Bibliothek, gekauft, so kann auch die Auslieferung der Waren online erfolgen.

- ***Elektronisches Rezept***
  Der Arzt könnte ein elektronisches Rezept erstellen, das entweder auf der Patientenkarte gespeichert wird oder an einen zentralen Apotheken-Rechner mittels HBCI übermittelt wird. Kommt der Patient zur Apotheke, so kann eine Zuzahlung mit einer HBCI-Überweisung oder bei kleineren Beträgen mit der Geldkartenfunktion auf der HBCI-Karte verwirklicht werden. Zur Abrechnung werden die entsprechenden Datensätze vom Apotheker kumuliert und per HBCI, evtl. in Kombination mit einer Lastschrift, bei der Krankenkasse eingereicht. Das Aufladen einer Geldkarte wird voraussichtlich als HBCI-Geschäftsvorfall in der HBCI-Version 3.0 enthalten sein.

4 Ein konkretes Beispiel – Elektronisches Ticket

Im vorherigen Kapitel führten wir als mögliches Anwendungsszenario die Buchung einer Zugreise mit HBCI an. Hier wollen wir einen konkreten Vorschlag für Geschäftsvorfälle zu diesem Zweck machen. Hier sei nochmals darauf hingewiesen, daß dieser Geschäftsfall ein Vorschlag unsererseits ist. Im Falle einer Standardisierung der X-HBCI Vorfälle durch das ZKA müßte dieser der dann vorgegebenen Maske angepaßt werden.

Die Buchung einer Zugreise würde sich in beispielsweise drei verschiedene Geschäftsvorfälle unterteilen lassen, die alle per HBCI durchgeführt werden könnten. Zunächst sollten die Buchungsdaten des gewünschten Ticket zur Bahn versendet werden. Ist für diese Fahrt eine Platzreservierung erwünscht, so sollte diese ebenfalls per HBCI übertragen werden können. Die anschließende Überweisung der entsprechenden Kosten an die Bahn schließt die Bestellung und Buchung des Bahnticket ab.
Soll ein HBCI-Geschäftsvorfall zu einem X-HBCI-Vorfall erweitert werden, so würde sich lediglich das Segment der HBCI-Nutzdaten ändern.[1]

4.1 Das gewünschte Ticket buchen

Die Buchungsdaten, die in dem Nutzdaten-Segment verarbeitet werden müssen, sollen folgende Details enthalten:

Gültigkeitszeitraum		
Art des Ticket	E	Einzelticket
	G	Gruppenticket
	W	Wochenendticket
	A	„Guten-Abend“-Ticket
Klasse	1, 2	
Start - Ziel		
Name des Buchenden		
Ermäßigung	25%, 50%, 75%. 100%	
Preis		
Währung	DEM, EURO, $US	
Wünsche zur Platzreservierung	R/N	Raucher/Nichtraucher
	Fen/Mit/Gan	Fenster/Mitte/Gang
	Tisch/-	Tischplatz
	Gro/Abt	Großraumwagen/Abteil

Abb.3: Dateninput für das Segment „Buchungsdaten“

[1] Die HBCI-Syntax einer Einzelüberweisung finden Sie im Anhang.

Das Segment „Buchungsdaten“ könnte demnach etwa folgendes Aussehen haben:

HBCI-Nutzdaten:

```
XHKBUC:4:2+12.12.98-14.12.98+E+Mz-Wi+1+MEIER
FRANZ+50++100,:DEM+51+000+R:Fen:Tisch:Gro´
```

XHKBUC:4:2	Segmentkopf „Buchungsdaten“
12.12.98-14.12.98	Gültigkeitszeitraum
E	Art des Tickets
Mz-Wi	Start – Ziel
1	Klasse
MEIER FRANZ	Name des Buchenden
50	Ermäßigung
100,	Preis
DEM	Währung
51	Textschlüssel, wie in den BPD festgelegt
000	Textschlüsselergänzung, zu Textschlüssel
R:Fen:Tisch:Gro	Platzreservierung

Abb.4: Buchungsdaten

4.2 Platzreservierung

Entsprechend den Buchungsdaten könnte sich auch das Segment „Platzreservierung“ gestalten. Bei der Platzreservierung seien etwa folgende Daten relevant:

Reisetag		
Zugnummer		
Klasse	1, 2	
Start – Ziel		
Name des Buchenden		
Preis		
Währung	DEM, EURO, $US	
Platzreservierung	R/N	Raucher/Nichtraucher
	Fen/Mit/Gan	Fenster/Mitte/Gang
	Tisch/-	Tischplatz
	Gro/Abt	Großraumwagen/Abteil
Wagennummer		
Sitzplatznummer		

Abb.5: Dateninput für das Segment „Platzreservierung“

Das Segment „Reservierung“ könnte demnach etwa folgendes Aussehen haben:

```
XHKRES:4:2+13.12.98+IC345+1+Mz-i+MEIER FRANZ++3,
+DEM+51+000+R:Fen:Tisch:Gro+12:83'
```

HBCI-Nutzdaten:

XHKRES:4:2	Segmentkopf „Reservierung“
13.12.98	Reisetag
IC345	Zugnummer
1	Klasse
Mz-Wi	Start – Ziel
MEIER FRANZ	Name des Buchenden
3,	Preis
DEM	Währung
51	Textschlüssel, wie in den BPD festgelegt
000	Textschlüsselergänzung, zu Textschlüssel
R:Fen:Tisch:Gro	Platzreservierung
12:83	Wagennummer – Sitzplatznummer

Abb.6: Platzreservierung

4.3 Kombinierte Ticketbestellung samt Platzreservierung

Um das Volumen der zu übertragenden gering zu halten, kann die Buchung des Ticket und die Platzreservierung miteinander verbunden werden. Daten, die für beide Geschäftsvorfälle relevant sind, würden somit nur einmal übertragen werden.

Ein Segment „Buchung&Reservierung“ könnte demnach etwa folgendes Aussehen haben:

HBCI-Nutzdaten:

```
XHKBUR:4:2+12.12.98-14.12.98+E+Mz-Wi+1+MEIER
FRANZ+50++100,:DEM+51+000+J+13.12.98+IC345+3,
:DEM+R:FEN:TISCH:GRO, 12:83+103,:DEM´
```

XHKBUR:4:2	Segmentkopf „Buchung&Reservierung“
12.12.98-14.12.98	Gültigkeitszeitraum
E	Art des Tickets
Mz-Wi	Start – Ziel
1	Klasse
MEIER FRANZ	Name des Buchenden
50	Ermäßigung
100,	Preis1
DEM	Währung
51	Textschlüssel, wie in den BPD festgelegt
000	Textschlüsselergänzung, zu Textschlüssel
J	Platzreservierung?
13.12.98	Reisetag

IC345	Zugnummer
3,	Preis2
DEM	Währung
R:Fen:Tisch:Gro	Platzreservierung
12:83	Wagennummer – Sitzplatznummer
103	Preis
DEM	Währung

Abb.7: Buchung und Platzreservierung

Es ist klar, daß in verschiedenen Bearbeitungsschritten Plausibilitätsprüfungen stattfinden müssen, um einen reibungslosen Ablauf zu gewährleisten. Die Überweisung des Betrages kann durch eine HBCI-Einzelüberweisung geschehen.

5 Ausblick

Hat sich HBCI erst einmal als Industriestandard innerhalb der deutschen Kreditwirtschaft etabliert, so wäre ein Fundament geschaffen, das sich die übrigen Wirtschaftszweige zu Nutzen machen könnten. Neue Geschäftsvorfälle, wie wir sie in Kapitel drei und vier angedeutet haben, könnten von Unternehmen und / oder Interessensgruppen in Abstimmung mit dem ZKA definiert werden. Es sollte ein einheitlicher noch nicht belegter Anfangsbuchstabe für X-HBCI reserviert werden. Um die Multibank-Fähigkeit von HBCI nicht auf's Spiel zu setzen darf die Unterstützung von X-HBCI Geschäftsvorfällen für "gewöhnliche" HBCI-Systeme nicht zwingend vorgeschrieben werden. Die Schaffung einer breiten Anwenderplattform X-HBCI würde für einzelne Unternehmen nicht nur Kosteneinsparungen, sondern - gerade in Verbindung von HBCI mit einer Geldkarte - auch einen enormen Funktionszuwachs bedeuten. Alltägliche Behördengänge, Einkäufe und Bankgeschäfte könnten dadurch stark vereinfacht werden.

Durch die Kopplung von HBCI mit anderen Mehrwert-Diensten könnte sich die Verbreitung von HBCI weiter steigern, was sicherlich im Interesse der deutschen Kreditwirtschaft sein dürfte. Somit wird HBCI auch die Kraft besitzen ein internationaler Standard zu werden.

Literatur:

[HBCIKOMP] Haubner, K.: „HBCI-Kompendium“, 1997, via http://members.aol.com/sxsigma/hbcikomp.pdf

[HBCISPEC] ZKA: „HBCI Spezifikation 2.01“, 1998, via http://www.siz.de/siz/hbci/hbcispec.htm

[HÜ98] Hühnlein, D.: „Die SmartCard-Algorithmen der nächsten Generation – Elliptische Kurven als RSA-Alternative“, in: CardForum, 3-98.

Anhang – Beispiel „Einzelüberweisung“

Hier sei das konkrete Aussehen einer HBCI-Nachricht anhand einer Einzelüberweisung beschrieben. Wie wir in Abbildung 2 gesehen haben, besteht eine HBCI-Nachricht aus verschiedenen ***Segmenten***. Auch der Nachrichtenkopf, der Signaturkopf, usw. bilden ein Segment. Ein Segment besteht wiederum aus verschiedenen ***Datenelementen***. Besteht ein Datenelement abermals aus mehreren logisch zusammengehörenden ***Gruppendatenelementen,*** so nennt man dieses Datenelement auch ***Datenelementgruppe***.[2] Das jeweils erste Datenelement eines Segmentes ist eigentlich eine Datenelementgruppe – der sog. ***Segment-Kopf***.

Grundsätzlich sieht HBCI folgende Trennzeichen vor:

+	Ende eines Datenelementes
:	Ende eines Gruppendatenelementes
‘	Ende eines Segmentes
?	Escape-Zeichen, falls im gewöhnlichen Text Trennzeichen benötigt werden
@	Kennzeichen für binäre Daten

Im folgenden sei die HBCI-Syntax am Beispiel einer Einzelüberweisung erläutert:

Nachrichtenkopf:

```
HNHBK:1:2+000000000315+201+4711+2‘
```

HNHBK	Segmentkennung „Nachrichtenkopf“
1	Segmentnummer, d.h. erstes Segment der Nachricht
2	Segmentversion
000000000315	Länge der gesamten Nachricht in Byte
201	HBCI-Version 2.01
4711	Dialog-ID
2	Nachrichten-Nummer innerhalb des Dialoges

Signaturkopf:

```
HNSHK:2:3 +1+765432+1+1+1::2+3234+1:19960701:
111144+1:999:1+6:10:16+280:10020030:76543:S:1:1
+<Zert>‘
```

HNSHK:2:3	Segmentkopf „Signaturkopf“
1	Sicherheitsfunktion „1“ für Non-Repudiation, wäre „2“ für Message Authentication bei DDH
765432	Sicherheitskontrollreferenz, hierauf bezieht man sich im Signaturabschluß

[2] Diese etwas „unkonventionell“ erscheinende Bezeichnungsweise ist in der HBCI-Spezifikation [HBCISPEC] definiert.

1	Bereich der Sicherheitsapplikation, d.h. welche Daten (bei Mehrfachsignaturen) in die Signatur einfließen, „1“ heißt es fließen nur Signaturkopf und HBCI-Nutzdaten ein.
1	Rolle des Sicherheitslieferanten, „1“ für Verfasser / Erstsignatur, wäre „2“ für Zweitsignatur oder „3“ für Zeuge, der nicht für den Inhalt der Nachricht verantwortlich ist.
1::2	Sicherheitsidentifikation (Details), „1“, da der Kunde etwas an die Bank sendet, mittleres leer, da RDH verwendet wird und „2“ für eine ID des Kundensystemes (optional)
3234	Sicherheitsreferenz-Nr., Sequenznummer von der Chipkarte bzw. vom Kundensystem generiert
1:19980817:181559	Datum und Uhrzeit, d.h. 17.08.1998, 18:15:59 Uhr
1:999:1	Hash-Algorithmus „RIPEMD-160“
6:10:16	Signatur-Algorithmus RSA
280	Ländercode
10020030	Bankleitzahl
76543	Benutzerkennung
S	Signierschlüssel, „V“ wäre Chiffrierschlüssel
1	Schlüsselnummer
1	Versionsnummer
<Zert.>	Transparent eingestelltes Zertifikat des Signaturschlüssels

Chiffrierkopf:

HNVSK:3:2
+4+1+1::1+1:19980817:191044+
2:2:13:@96@*<chiffrierter Schlüssel>*:6:1+

HNVSK:3:2	Segmentkopf „Chiffrierkopf“
4	Sicherheitsfunktion „4“ für Verschlüsseln
1	Rolle des Sicherheitslieferanten „1“ für Erfasser, „4“ für Zeuge
1::1	Sicherheitsidentifikation, s.o.
1:19980817:191044	Datum und Uhrzeit, s.o.
2	Verwendung des Verschlüsselungsalgorithmus „2“ für symmetrisch
2	Operationsmodus, „2“ für CBC
13	Verschlüsselungsalgorithmus, „13“ für 2-Key-Triple-DES
@96@<Chiffrierter Schl.>	Mit RSA verschlüsselter Triple-DES-Key
6	Schlüsselbezeichner, „6“ für RSA verschlüsselter Triple-DES-Key, „5“ für mit Triple-DES verschlüsselter Triple-DES-Key (für DDV)
1	Bezeichner für Initialisierungsvektor, zur Zeit ist nur 0.. zulässig

280:10020030:12345:V:1:1	Schlüsselname, s.o.
0	Kompressionsalgorithmus, „0“ für keine Kompression, andere siehe [HBCISPEC], Teil B, Seite 38
<Zert.>	Transparent eingestelltes Zertifikat des RSA-Verschlüsselungs-Schlüssels

HBCI-Nutzdaten:

HKUEB:4:2+1234567:280:10020030+7654321:280:20030040+MEIER FRANZ++1000,:DEM+51+000+RE-NR.1234:KD-NR.9876'

HKUEB:4:2	Segmentkopf „Einzelüberweisung“
1234567:280:10020030	Kontoverbindung Auftraggeber
7654321:280:20030040	Kontoverbindung Empfänger
MEIER FRANZ	Name des Empfängers
1000,	Betrag
DEM	Währung
51	Textschlüssel, wie in den BPD festgelegt
000	Textschlüsselergänzung, zu Textschlüssel
RE-NR.1234:	Verwendungszweck 1
KD-NR.9876	Verwendungszweck 2

HBCI-Nutzdaten (verschlüsselt):

HNVSD:4:1+@74@*<Daten, verschlüsselt>*

HNVSD:4:1	Segmentkopf „Verschlüsselte Daten“
@74@...	74 Byte, verschlüsselte Daten

Signaturabschluß:

HNSHA:5:1+765432+@96@<*Signatur*>

HNSHA:5:1	Segmentkopf „Signaturabschluß“
765432	Sicherheitsreferenznummer, referenziert Signaturkopf
@96@...	RSA-Signatur

Nachrichtenabschluß:

HNHBS:6:1

HNHBS:6:1	Segmentkopf „Nachrichtenabschluß“
2	Nachrichtennummer, referenziert Nachrichtenkopf