

## HBCI / FinTS



### BASISWISSEN

#### Sicherheits-Verfahren für Banking-Programme

**Wenn Sie beim Online-Banking ein Zahlungsverkehrs-Programm verwenden, etwa die VR-Networld Software, senden Sie Ihre Daten mit Hilfe des Sicherheits-Standards „HBCI/FinTS“ an Ihre Bank. Lesen Sie, was dieses Kürzel bedeutet.**

#### Zum Verständnis

Banking über die Internet-Seite

Wer vom Online-Banking spricht, meint in der Regel das so genannte browser- oder internet-basierte Banking. Hierbei gehen Sie mit Hilfe Ihres Browsers, zum Beispiel mit dem Internet-Explorer, auf die Internet-Seite Ihrer Bank und wählen sich mit Ihren Zugangsdaten in die Banking-Anwendung ein.

Banking mit Finanz-Software

Eine zweite Variante bezeichnen Experten als software-basiertes Online-Banking. Dazu installieren Sie ein Banking-Programm auf der Festplatte Ihres Computers, beispielsweise die VR-NetWorld Software. Ihre Daten tauscht das Programm mit Hilfe des HBCI/FinTS-Standards mit dem Bankrechner aus. Dieser Beitrag handelt vom software-basierten Banking.

Technischer Standard für das Online-Banking

#### HBCI / FinTS

Das Kürzel „HBCI“ steht für „**Homebanking Computer Interface**“. Gemeint ist ein Computer-Standard, mit dessen Hilfe beispielsweise eine Überweisung in verschlüsselter Form über das Internet versendet werden kann. Diesen technischen Standard hat die deutsche Kreditwirtschaft in den neunziger Jahren entwickelt. Alle Bankengruppen, die der Zentrale Kreditausschuss (ZKA) repräsentiert, unterstützen den HBCI-Standard. Im ZKA ist unter anderem der Bundesverband der Deutschen Volksbanken Raiffeisenbanken (BVR) vertreten.

### Verschlüsselung von Aufträgen

Zentral festgelegt sind im HBCI-Standard

- zum einen die Art und Weise, wie ein Auftrag, den der Kunde an die Bank schickt, verschlüsselt wird und wie die Identitäten von Kunde und Bank nachgewiesen werden (Authentifizierung), und
- zum anderen ist der Ablauf einzelner Bankgeschäfte wie zum Beispiel einer Überweisung klar definiert.

### Neue Möglichkeiten

Im Jahr 2002 ist HBCI im „**Financial Transaction Service**“ (FinTS) aufgegangen. Dieser Standard bietet gegenüber den HBCI-Vorgängern zusätzliche Möglichkeiten: So können Online-Überweisungen seitdem nicht nur mit der generell üblichen elektronischen Signatur, sondern auch mit dem Sicherheits-Verfahren PIN/TAN beauftragt werden. Mehr Sicherheit gibt es beim FinTS-Standard, weil mit ihm die verwendeten elektronischen Schlüssel verlängert wurden - von 1024 auf 2048 Bit.

## Digitale Signatur

### Ein Baukasten mit vielen Möglichkeiten

Der FinTS-Standard gleicht einem Baukasten, in dem verschiedene Sicherheits-Verfahren angewendet werden können. Das von den Volksbanken Raiffeisenbanken überwiegend eingesetzte Verfahren ist das RSA-Verfahren, benannt nach seinen Erfindern Ronald **R**ivest, Adi **S**hamir und Leonard **A**dleman.

### Das RSA-Verfahren

Kurz formuliert funktioniert es so: Wenn der Nutzer mit dem Banking-Programm eine Überweisung an seine Bank sendet, schickt er ihr zeitgleich mit dem Auftrag einen digitalen Schlüssel – eine Zahlen-Kolonne, die nur die Bank entschlüsseln kann. Auch die Bank sendet während des Banking-Dialogs dem Kunden einen Schlüssel, so dass sich beide Partner gegenseitig als vertrauenswürdig authentifizieren. Erst wenn dies gewährleistet ist, wird der Auftrag ausgeführt. Beim Kunden ist der Schlüssel entweder in einer Datei oder auf einer Chipkarte, der VR-NetWorld-Card, gespeichert.

Ausführlich beschrieben ist das RSA-Verfahren im Handbuch zur VR-NetWorld Software.

## Sicherheit

### Die VR-NetWorld-Card

Die VR-NetWorld-Card ähnelt optisch der VR-BankCard, hat allerdings eine ganz andere Funktion. Im Chip dieser Karte ist die Signatur gespeichert, die für die Verschlüsselung der Kommunikation zwischen dem PC des Kunden und dem Rechner der Bank notwendig ist. Da die wenigsten Windows-Computer ein entsprechendes Laufwerk haben, schließt der Kunde ein Karten-Lesegerät am Computer an. Für die VR-NetWorld Software ist ein Kartenleser der Klasse 2 oder 3 erforderlich.

### Drei gute Gründe

HBCI/FinTS mit Chipkarte gilt als eines der sichersten Banking-Verfahren, da

- der Nutzer den digitalen Schlüssel nur mit seinem persönlichen Kennwort aktivieren kann,
- dieser Schlüssel den Speicherplatz nie verlässt und auch nicht kopiert werden kann und
- der Nutzer bei Kartenlesern der Klasse 2 und 3 die PIN nicht über die Computer-Tastatur eingibt, sondern in die Tastatur des Kartenlesers.

### Vorsicht mit sensiblen Daten

Ebenso sorgfältig, wie Sie beim browser-basierten Online-Banking Ihre Zugangsdaten und Ihre Transaktions-Nummern (TAN) handhaben, sollten Sie auch beim Banking mit Software darauf achten, dass niemand Ihre Zugangsdaten oder Ihre Diskette oder Chipkarte in die Hände bekommt. Bewahren Sie deswegen niemals Ihr Sicherheits-Medium und die Passwörter an einem Ort auf.

Wenn Sie Interesse an der VR-NetWorld Software haben, sprechen Sie mit Ihrem Berater. Bei ihm erhalten Sie alle weiteren Informationen.