Leitfaden HBCI/FinTS

Inhaltsverzeichnis

1. Einleitung - Was ist HBCI/FinTS?

Mit HBCI (Home Banking Computer Interface) haben die Verbände der deutschen Kreditwirtschaft in Zusammenarbeit mit dem Zentralen Kreditausschuss einen Standard für die Kommunikation zwischen Bankrechnern und Kundenprodukten (wie Kontenauszugsmanager) definiert. Die Kommunikation erfolgt über das Internet.

Für den Schutz der Daten werden elektronische Signaturen / Unterschriften bei der Kommunikation zwischen dem Bankrechner und dem Kundenprodukt ausgetauscht.

Der HBCI-Standard wird regelmäßig vom Zentralen Kreditausschuss weiterentwickelt. Seit der HBCI-Version 3.0 wird dieser Standard FinTS genannt. FinTS ist die Abkürzung für Financial Transaction Service. Auf dem Markt sind verschiedene HBCI/FinTS-Versionen vertreten. Die Einführung und Unterstützung der jeweiligen Version liegt in der Entscheidungsgewalt der einzelnen Bank.

Ihre Bank hat spezielle Sicherheitsmedien und -daten für den HBCI-Zugang. Alle sicherheitsrelevanten Medien und Daten sollen an einem sicheren Ort aufbewahrt werden.

2. Was wird für Homebanking über HBCI/FinTS benötigt?

Nachfolgende Informationen und Voraussetzungen müssen vorhanden sein, um Homebanking mit ihrer Bank machen zu können.

- Internet Zugang
- Freischaltung ihrer Bank für Homebanking über HBCI
- Internet-Adresse ihrer Bank
- Bankleitzahl ihrer Bank. Die Bankleitzahl für HBCI kann von der Bankleitzahl der Filiale abweichen.
- HBCI-Benutzerkennung von ihrer Bank
- HBCI-Kunden-ID von ihrer Bank. Die Kunden-ID für HBCI kann von der üblichen Kundennummer abweichen.
- unterstützte HBCI/FinTS Version ihrer Bank

Es sind außerdem die System- und Hardwarevoraussetzungen zu beachten.

2.1. System- und Hardwarevoraussetzungen

Die Systemvoraussetzungen sind im Dokument <Systemvoraussetzungen SBS Rewe neo®.pdf> beschrieben. Für die Lauffähigkeit von Sicherheitsmedien wie z.B. einem Chipkartenlesegerät kann es spezielle Systemvoraussetzungen geben. Informieren Sie sich bitte bei den entsprechenden Herstellern und Verkaufsstellen.

3. Wie wird HBCI/FinTS genutzt?

Für jede Bank wird ein Homebanking-Kontakt eingerichtet, der über den Kontenauszugsmanager verwaltet wird. Ggf. sind mehrere Homebanking-Kontakte bei einer Bank notwendig.

Der Homebanking-Kontakt wird nach Bereitstellung der Zugangsdaten durch ihre Bank im Programm angelegt und synchronisiert, d.h. es wird eine Zugangsberechtigung und eine Identifikation mit dem Benutzer vorgenommen. Das Programm verwaltet die Homebanking-Kontakte automatisch.

Für die Kommunikation mit dem Bankrechner müssen die Sicherheitsmedien und die Passwörter zum Zeitpunkt der Übertragung zur Verfügung stehen.

Bei der Beantragung des HBCI-Zugangs muss mind. die **Kontoabfrage** von ihrer Bank freigeschaltet werden. Nur mit dieser Freischaltung kann der Kontenauszugsmanager elektronische Kontoumsätze abholen.

Bevor der HBCI-Zugang genutzt werden kann, muss mittels der Sicherheitsmedien und -verfahren der Kontakt synchronisiert werden. Diese Funktionalität befindet sich im Kontenauszugsmanager unter HBCI Verwaltung mit der Funktion Kontakt synchronisieren. Erst wenn der Homebanking-Kontakt erfolgreich synchronisiert wurde, kann der HBCI-Zugang vollständig genutzt werden.

4. Sicherheitsmedien und -verfahren

Für eine eindeutige Identifikation des Kunden beim Bankrechner und für die Verschlüsselung der Daten werden verschiedene Sicherheitsmedien/Sicherheitsverfahren durch die Banken unterstützt.

4.1. Schlüsseldatei

Ihre Bank stellt Ihnen bankspezifische Zugangsdaten zur Verfügung. Bei der Bereitstellung von Zugangsdaten werden ein so genannter INI-Brief und Sicherheitsdateien erstellt. Für den vollständigen Zugang zum Bankrechner muss der INI-Brief unterschrieben an die Bank zurückgegeben werden. Die Freischaltung erfolgt dann durch die Bank.

Der Speicherort der Sicherheitsdateien kann auf einer Diskette/USB Stick (eine oder mehrere Banken), mehreren Disketten/USB-Sticks (mehrere Banken) oder auf der Festplatte (eine oder mehrere Banken) sein.

4.2. Sicherheitsmedium Chipkarte

Ihre Bank stellt Ihnen eine Chipkarte mit vorbereiteten Sicherheitsdateien und i.d.R. einen Chipkartenleser zur Verfügung. Ein Chipkartenleser muss an das System angeschlossen und in Betrieb genommen werden. Die Vorgehensweise für die Inbetriebnahme entnehmen Sie bitte der Beschreibung des Chipkartenlesers. Auf einer Chipkarte können auch mehrere Banken eingerichtet werden.

4.3. Sicherheitsverfahren PIN / TAN-Verfahren

Ihre Bank stellt Ihnen eine PIN (Persönliche Identifikationsnummer) und eine TAN-Liste (auch TAN-Bogen genannt) mit einer Anzahl von TAN´s (Transaktionsnummern) zur Verfügung. Die PIN ist die Zugangsberechtigung des Kontos zum Bankrechner. Mit dieser PIN können elektronische Kontoumsätze abgeholt werden. Die TAN ist eine elektronische Unterschrift für die Ausführung von Zahlungsaufträgen.

Aktuelle Entwicklungen im Bereich des PIN/Tan-Verfahren sind die Einführung von iTAN (indizierte TAN) und mTAN (mobile TAN). Bei iTAN muss eine von der Bank angefragte bestimmte TAN-Nr. benutzt werden. Bei MTAN erhalten Sie die TAN per SMS oder speziellem Empfangsgerät für die Transaktion von der Bank übermittelt.

Hinweis: Eine Beratung über den Einsatz, der Realisierung und den Kosten von Sicherheitsmedien und -verfahren erhalten Sie bei ihrer Bank.