Homebanking-Verfahrensanleitung

Stand: Mai 2006

1 Technische Voraussetzungen beim Nutzer

Der Nutzer (Kontoinhaber und etwaige Bevollmächtigte) benötigt ein Online-Banking-fähiges Endgerät (Kundensystem). Dieses Kundensystem kann insbesondere sein:

- ein internetfähiger PC mit installierter Online-Banking-Software, gegebenenfalls einem Chipkartenleser und einem Modem oder einer ISDN-Karte;
- ein internetfähiger PC mit installiertem Internet-Browser, gegebenenfalls einem Chipkartenleser und einem Modem oder einer ISDN-Karte;
- ein sonstiges internetfähiges Endgerät mit entsprechender Ausstattung mit Chipkartenleser (z. B. Smartphone).

Darüber hinaus benötigt der Nutzer den Zugang zu einem Telekommunikationsnetz (z. B. Telefonanschluss) und gegebenenfalls zu einem Online-Dienst (z. B. Internetzugang). Über die hierfür vom Nutzer zu zahlenden Entgelte kann dieser sich bei den entsprechenden Anbietern informieren.

2 Funktion des Kundensystems

Mit dem Kundensystem können verschiedene Nachrichten erzeugt werden, wie z. B. die Erteilung von Aufträgen für den Inlands- und Auslandszahlungsverkehr, die Abholung von Konto- und Umsatzinformationen oder Statusprotokollen sowie die Initialisierung der Verbindung. Diese Nachrichten werden online an das Kreditinstitut übermittelt.

Hinweise zur Nutzung der Online-Banking-Funktionen können

- beim Online-Banking per Internetbrowser vom Kundensystem angezeigt und /oder beim Kreditinstitut erfragt werden;
- bei Nutzung einer Online-Banking-Software dem vom Hersteller des Kundensystems gelieferten Benutzerhandbuch entnommen werden.

3 Sicherungsverfahren

Zum Schutz der elektronischen Datenübermittlung zwischen Nutzer und Kreditinstitut werden die im Folgenden beschriebenen Sicherungsverfahren eingesetzt:

- Durch Verschlüsselung werden die zu übertragenden Nachrichten gegen Einsicht durch unberechtigte Dritte geschützt.
- Durch Verfahren zur elektronischen Signatur werden die Inhalte und der Ursprung von Nachrichten gegen Fälschung gesichert.

Das elektronische Signaturverfahren verwendet geheime Schlüssel. Diese Schlüssel werden entweder

- vom Kreditinstitut in einer Chipkarte sicher gespeichert an den Nutzer ausgeliefert oder
- vom Nutzer für sich selbst generiert.

Der geheime Schlüssel dient der Erzeugung der elektronischen Signatur und damit zur Autorisierung von Aufträgen oder zur Abfrage von Informationen des Kontoinhabers gegenüber dem Kreditinstitut durch den jeweiligen Nutzer. Der geheime Schlüssel verbleibt beim Nutzer und ist sicher vor dem Zugriff Unbefugter aufzubewahren.

Der geheime Schlüssel kann in einem der folgenden Signaturmedien gespeichert sein:

a) HBCI-Chipkarte oder Bank-Karte mit Signaturfunktion

Der Nutzer erhält vom Kreditinstitut eine Chipkarte mit allen erforderlichen Zugangsdaten des Kreditinstituts sowie eine Transport-PIN (Geheimnummer) für die Karte. Mit Hilfe der Transport-PIN legt der Nutzer eine HBCI-PIN zum Zugriff auf die Karte fest, die nicht identisch mit der PIN der Bank-Karte ist.

b) Unpersonalisierte HBCI-Chipkarte oder Token zum Erzeugen von Signaturen

Der Nutzer erhält vom Kreditinstitut eine Chipkarte oder ein ähnliches elektronisches Gerät (Token), das bei der Auslieferung nicht personalisiert ist und keine PIN enthält. Vor dem ersten Einsatz muss der Nutzer daher zuerst folgende Schritte ausführen:

- Der Nutzer gibt in seinem Kundensystem die Zugangsdaten (Kunden-ID, Kommunikationszugänge) ein, die er von seinem Kreditinstitut erhalten hat. Das Kreditinstitut übermittelt dem Kundensystem seinen öffentlichen Schlüssel, den der Nutzer mit den Zugangsdaten vergleichen muss, die er von dem Kreditinstitut erhalten hat.
- Die Karte generiert die erforderlichen Schlüssel. Der Nutzer legt eine HBCI-PIN zum Zugriff auf die Karte fest. Mit seinem Kundensystem übermittelt der Nutzer seine öffentlichen Schlüssel an das Kreditinstitut und erstellt ein Initialisierungsprotokoll (Ini-Brief). Diesen Ini-Brief unterschreibt er persönlich und schickt ihn an das Kreditinstitut.
- Das Kreditinstitut erhält den Ini-Brief und vergleicht diesen mit den vorher elektronisch erhaltenen Schlüsseln des Nutzers. Nach positiver Prüfung schaltet das Kreditinstitut das Signaturmedium des Nutzers für das Online-Banking frei.

c) beliebiges Speichermedium (HBCI-Software-Version)

Hierfür wählt der Nutzer ein beliebiges beschreibbares Speichermedium, wie z. B. eine Diskette. Das Kundensystem erzeugt auf diesem Medium die Schlüssel des Nutzers. Für die Erzeugung werden die gleichen Schritte wie unter b) durchgeführt.

Zur Prüfung der Signatur des Nutzers benötigt das Kreditinstitut ebenfalls Schlüssel, die mit dem Nutzer vereinbart werden. Diese sind entweder

- als geheim zu haltender Schlüssel mit dem Schlüssel des Kunden identisch oder
- werden als öffentlicher Schlüssel des Kunden im Zuge der Initialisierung an das Kreditinstitut übermittelt.

Die Schlüssel des Nutzers können auch für die Kommunikation mit anderen Kreditinstituten eingesetzt werden (Multibankfähigkeit), wenn dies mit einem anderen Kreditinstitut vereinbart wird. Gegebenenfalls müssen hierfür die gleichen Schritte wie unter b) durchgeführt werden.

4 Auftragserteilung oder Abfrage von Informationen

Der Nutzer wählt die von ihm gewünschte Funktion in seinem Kundensystem aus und erfasst die für die Nachrichtenübermittlung erforderlichen Daten. Er überprüft die zu signierenden Aufträge auf Richtigkeit.

Diese Nachrichten versieht der Nutzer mit einer elektronischen Signatur. Hierzu verwendet er sein Identifikations- und Legitimationsmedium und gibt sein Passwort ein. Falls mehrere elektronische Signaturen pro Auftrag mit dem Kreditinstitut vereinbart sind, ist der Signiervorgang je signaturpflichtigem Nutzer entsprechend zu wiederholen.

Die signierten Nachrichten werden dann online an das Kreditinstitut übertragen.

Das Kreditinstitut wird eine empfangene Nachricht nur dann bearbeiten, wenn sie die erforderliche Anzahl von ordnungsgemäßen elektronischen Signaturen enthält.

Das Kreditinstitut bestätigt im elektronischen Dialog den Eingang von Aufträgen durch Übersendung einer Empfangsbestätigung oder übermittelt die angefragten Daten.

Der Nutzer kann sich zu einem späteren Zeitpunkt durch Abruf eines Statusprotokolls über die Ausführung des Auftrags informieren, wenn er vor dem Versenden der Auftragsnachricht unterbrochen wurde.