

# Verfahrensanleitung für Online-Banking mit TAN-Generator

Stand: Dezember 2004

## 1 Technische Voraussetzungen beim Nutzer

Der Nutzer (Kontoinhaber und etwaige Bevollmächtigte) benötigt ein onlinebankingfähiges Endgerät (Kundensystem). Dieses Kundensystem kann insbesondere sein:

- ein internetfähiger PC mit installierter Online-Banking-Software;
- ein internetfähiger PC mit installiertem Internetbrowser;
- ein sonstiges internetfähiges Endgerät mit entsprechender Ausstattung (z. B. PDA, Mobiltelefon).

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 von dem Nutzer zu zahlenden Entgelte kann er sich bei den entsprechenden Anbietern informieren.

Zusätzlich benötigt der Benutzer einen TAN-Generator, den er von seinem kontoführenden Institut erhält. Dieser besteht in der Regel aus einer Bankchipkarte mit TAN-Generatorapplikation und einem TAN-Chipkartenleser als Anzeigemodul.

## 2 Funktion des Kundensystems

Mit dem Kundensystem können verschiedene Nachrichten erzeugt werden, wie die Erteilung von Aufträgen z. B. für den Inlands- und Auslandszahlungsverkehr, die Abholung von Konto- und Umsatzinformationen oder Statusprotokollen sowie die Initialisierung. 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 wird das im Folgenden beschriebene Authentisierungsverfahren eingesetzt:

- Durch die Eingabe seiner Kontonummer bzw. seines individuell gewählten Anmeldenamens<sup>1</sup> und einer Persönlichen Identifikationsnummer (PIN) legitimiert sich der Benutzer gegenüber dem Kreditinstitut.
- Durch die Eingabe einer einmalig gültigen Transaktionsnummer (TAN) wird der Inhalt und der Ursprung von Nachrichten gesichert und autorisiert.
- Die Online-Banking-Software bzw. der Internetbrowser verschlüsselt die zu übertragenden Nachrichten, sodass sie gegen Einsicht durch unberechtigte Dritte geschützt sind.

Nach der Anmeldung hat der Nutzer Zugriff auf das jeweilige Online-Konto bzw. alle Online-Konten des zugehörigen Kontenverbundes<sup>1</sup>. Nachdem der Nutzer sich mit dem zugewiesenen Anmeldenamen angemeldet hat, kann er diesen beliebig ändern, sofern der gewählte Anmelde-name nicht bereits an andere Nutzer vergeben ist.

Beim Erstzugang muss der Nutzer seine PIN ändern. Dabei muss die vom Kreditinstitut zugewiesene PIN auf eine persönliche PIN geändert werden. Andere Transaktionen sind vorher nicht möglich.

Der Nutzer kann darüber hinaus seine PIN auf eigenen Wunsch (z. B. bei Verdacht auf Kompromittierung) ändern. Die PIN-Änderung wird vom

Nutzer durch Eingabe einer gültigen TAN bestätigt. Nach Änderung der PIN kann die alte PIN nicht mehr verwendet werden.

Wird dreimal hintereinander eine falsche PIN eingegeben, so wird der Online-Zugang zum Konto gesperrt. Der Nutzer kann auch auf eigenen Wunsch seine PIN bzw. das Konto mit Hilfe einer Online-Banking-Transaktion sperren. Danach ist ein Online-Zugang zum Konto nicht mehr möglich. Der Nutzer kann diese Sperre per Online-Banking-Transaktion aufheben, indem er neben der richtigen PIN eine gültige TAN eingibt.

Aus Sicherheitsgründen dürfen weder die PIN noch die TANs im Kundensystem gespeichert 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 freizugebenden Aufträge auf Richtigkeit.

Diese Nachrichten autorisiert der Nutzer mit einer Transaktionsnummer (TAN). Hierzu verwendet der Nutzer seine Bankchipkarte. Die so im Chip der Karte errechnete TAN wird anschließend im Display des TAN-Generators angezeigt. Der Nutzer trägt die TAN in das hierfür vorgesehene Feld im Internetbrowser oder der Online-Banking-Software ein.

Zum Zwecke der Nachverfolgung sollte der Nutzer vermerken, für welche Transaktion welche TAN verwendet wurde. Eine erzeugte TAN ist so lange gültig, bis eine danach erzeugte TAN beim Kreditinstitut eingereicht wurde. Nach Einreichung und Verarbeitung der TAN beim Kreditinstitut kann diese nicht mehr genutzt werden. Es können auch TANs übersprungen werden, d. h. erzeugt, aber nicht beim Kreditinstitut eingereicht werden. Hierbei ist jedoch zu berücksichtigen, dass bei zu häufigem Überspringen TANs eventuell nicht mehr als gültig erkannt werden können und der TAN-Generator somit kreditinstitutsseitig gesperrt wird (siehe unten).

Falls mehrere Transaktionsnummern pro Auftrag mit dem Kreditinstitut vereinbart sind, ist dieser Vorgang je berechtigtem Nutzer entsprechend zu wiederholen. Die mit TANs autorisierten Nachrichten werden dann online an das Kreditinstitut übertragen.

Gibt der Nutzer dreimal hintereinander eine falsche TAN ein, so wird der TAN-Generator für die Verwendung am Konto gesperrt. Der Nutzer kann dann nur noch Geschäftsvorfälle ausführen, die keine TAN erfordern.

Kann der Transaktionszähler (ATC) der Karte vom kontoführenden Institut nicht automatisch erkannt werden und ist der TAN-Generator nicht gesperrt, besteht die Möglichkeit, die Funktionsfähigkeit des TAN-Generators durch Eingabe des ATC und einer gültigen TAN wieder herzustellen. Dazu liest der Nutzer den aktuellen ATC der Karte mit dem TAN-Chipkartenleser aus und sendet ihn zusammen mit der richtigen TAN mit einer speziellen Transaktion an das Kreditinstitut. Kann der TAN-Generator so nicht synchronisiert werden, muss sich der Nutzer mit seinem Kreditinstitut persönlich in Verbindung setzen.

Das Kreditinstitut wird eine empfangene Nachricht nur dann bearbeiten, wenn sie die erforderliche Anzahl von ordnungsgemäß eingereichten TANs enthält. Das Kreditinstitut bestätigt im elektronischen Dialog den Eingang von Aufträgen durch Übersendung einer Empfangsbestätigung oder übermittelt die angefragten Daten.

<sup>1</sup> Nichtzutreffendes bitte streichen.