

Software: Profi Cash

HBCI-Leitfaden

1. Internet-Konfiguration für die HBCI Kommunikation

Der Datenaustausch per HBCI wird über das Internet durchgeführt. Für den Zugang ins Internet muss eine der folgenden Bedingungen erfüllt sein:

- das DFÜ Netzwerk mit einem Eintrag ihres Providers ist installiert.
- es besteht eine ständige Internetverbindung (z.B. über Router / LAN).
- die Verbindung wird vor jeder HBCI-Übertragung manuell hergestellt.
- eine AOL-Software ist installiert.
- es ist ein lokales Netzwerk mit einem HTTP Proxyserver vorhanden.
- es ist ein lokales Netzwerk mit einem Socks 5 Proxyserver vorhanden.

Ist das DFÜ-Netzwerk installiert, wählen Sie unter dem Menü "Einstellungen - Internetzugang" den Knopf "DFÜ-Netzwerk" und den gewünschten Eintrag aus. Mit dem gewählten Eintrag wird dann jeweils automatisch eine Verbindung hergestellt.

Sollte eine ständige Internetverbindung vorhanden oder bereits zuvor hergestellt worden sein, wählen Sie unter dem Menü "Einstellungen - Internetzugang" den Knopf "manuell ohne Meldungen (z.B. über Router / LAN)". In diesem Fall wird direkt auf eine bestehende Verbindung aufgesetzt.

Möchten Sie die Internetverbindung jeweils manuell starten und beenden, wählen Sie unter dem Menü "Einstellungen - Internetzugang" den Knopf "manuell mit Meldungen". In diesem Fall erfolgt vor und nach jeder Übertragung die Aufforderung die Verbindung herzustellen bzw. zu beenden.

Für einen Zugang zum Internet über AOL wählen Sie bitte den Knopf "AOL", vor einer HBCI Datenübertragung wird dann die AOL-Software gestartet, eine Verbindung aufgebaut und nach der Datenübertragung wieder beendet.

Wenn Sie die Internetverbindung über ein lokales Netzwerk und einen sogenannten HTTP Proxyserver oder Socks 5 Proxyserver herstellen wollen, wählen Sie den Knopf "HTTP Proxy" bzw. "Socks 5 Proxy". Zusätzlich müssen Sie dann die Adresse und den Anschluss Ihres Proxyservers angeben. Sofern eine Legitimierung am Proxyserver erforderlich ist, wird der Benutzername und das Kennwort vor dem Verbindungsaufbau abgefragt. Bei Fragen zu den Proxyeinstellungen, wenden Sie sich bitte an Ihren Netzwerk-Administrator.

Möchten Sie nach einer HBCI Datenübertragung über das DFÜ-Netzwerk oder AOL gelegentlich die Internetverbindung aufrecht erhalten, können Sie die Option "Rückfragen vor Verbindungsabbau" aktivieren. Sie werden dann an entsprechender Stelle gefragt, ob die Verbindung bestehen bleiben soll. Bestätigen Sie diese Frage mit "Ja", so müssen Sie die Internetverbindung später selber manuell beenden.

2. Anlage eines HBCI Zugangs

Der Einstieg in die HBCI-Verwaltung ist über das Menü "Stammdaten - HBCI-Verwaltung" oder aus dem Kontenstamm über den Button "HBCI-Verwaltung..." heraus möglich. Beim erstmaligen Programmstart wird automatisch in diese Maske verzweigt.

Abhängig von Ihrer Bank gibt es grundsätzlich zwei verschiedene Möglichkeiten, auf welche Art Ihre sicherheitsrelevanten HBCI Daten gespeichert werden: Entweder auf einer durch das Zahlungsverkehrsprogramm erstellten Diskette/USB-Stick (GLS Bank-Verfahren, HBCI Sicherheitsdatei, Abschnitt 3) oder auf einer HBCI Chipkarte (Abschnitt 4), die Ihnen durch Ihre Bank zur Verfügung gestellt wird.

Weiterhin unterstützen viele Banken inzwischen das so genannte PIN/TAN-Interface. (Abschnitt 5)

3. HBCI Sicherheitsdatei

3.a) Lesen einer HBCI Sicherheitsdatei

Wenn Ihnen bereits eine HBCI Sicherheitsdatei zur Verfügung steht, können Sie diese einlesen und im Programm nutzen. Falls Sie die Sicherheitsdateien nicht auf einer Diskette/USB-Stick verwalten, muss die Datei zunächst in das unter "Verzeichnis für Sicherheitsdateien" angegebene Verzeichnis kopiert werden. Nach Betätigung des Buttons "Sicherheitsdatei lesen" öffnet sich ein Dateiauswahlfenster in dem die zu übernehmende Sicherheitsdatei auszuwählen ist.

Anschließend werden Sie nach der ID bzw. dem Benutzernamen der Sicherheitsdatei gefragt. Bei durch Profi cash erstellten Sicherheitsdateien entspricht diese ID/Benutzername der 8-stelligen Ziffernfolge, die den Dateinamen bildet. Diese ID/Benutzername wird beim Lesen der Sicherheitsdatei daher auch vorgeschlagen. Wurde die Sicherheitsdatei mit einem anderen Programm erstellt, so sind ID/Benutzername und Dateiname in der Regel nicht identisch. In diesem Fall ist die ID/Benutzername dem Programm zu entnehmen, mit dem die Datei erstellt wurde.

Aus der Sicherheitsdatei werden dann Benutzerkennung, Bankleitzahl und die Internet-Adresse der Bank gelesen, das HBCI-Kürzel kann wie beim Neu Erstellen einer Sicherheitsdatei frei gewählt werden. Auch der Status der Sicherheitsdatei wird natürlich übernommen, so dass Sie mit einer vorher bereits erfolgreich initialisierten Datei sofort arbeiten können.

3.b) Erstellen einer HBCI Sicherheitsdatei

Aus der "HBCI-Verwaltung" gelangen Sie über die Taste "Neu..." oder "Bearbeiten..." zur manuellen Anlage neuer HBCI Zugänge. Tragen Sie hier ein beliebiges HBCI-Kürzel ein (Empfehlung: Bankname+Nachname="GLSMÜLLER"), unter dem das Programm den HBCI-Zugang in Zukunft identifiziert.

Unter Sicherheitsmedium/-verfahren wählen Sie "Sicherheitsdiskette / Sicherheitsdatei".

Die Bankleitzahl, die Benutzerkennung und die Kundennummer/-ID wurden Ihnen von Ihrer Bank auf dem HBCI-INI-Brief mitgeteilt. Bei genossenschaftlichen Instituten sind Benutzerkennung und Kundennummer/-ID identisch. Achten Sie auf die exakte Schreibweise (einschließlich der Groß- und Kleinschreibung) dieser Daten!

Die Sicherheitsdatei wird durch ein Passwort geschützt. Die Speicherung dieses Passwortes ist zwar möglich, sollte aber da dies ein Sicherheitsrisiko darstellt, nicht genutzt werden. Wird bei den HBCI-Parametern kein Passwort hinterlegt, so wird es vor jeder Übertragung abgefragt. Das Passwort muß mindestens 8 Zeichen lang sein und mindestens eines der Sonderzeichen . < > () + - & ? * ; , % : " ' = enthalten.

Unter "Internet-Adresse" tragen Sie bitte, sofern die Adresse nicht automatisch vorgeschlagen wird, die HBCI-Internet-Adresse ein, die Ihnen ebenfalls von Ihrer Bank mitgeteilt wurde (GLS = hbc.gad.de).

Nach dem Speichern dieser Daten wird geprüft, ob bereits eine Bankparameterdatei (BPD) der Bank vorliegt, um die aktuell unterstützte HBCI-Version sowie die zu benutzende Schlüssellänge (zwischen 768 und 2048 Bit) zu ermitteln. Ist das nicht der Fall, wird diese Datei zunächst in einem anonymen Dialog bei der Bank angefordert. Erst jetzt kann ein neues Sicherheitsmedium angelegt werden.

3.c) Initialisieren der HBCI-Sicherheitsdatei

Daraufhin werden Ihre persönlichen Schlüssel generiert und in der Sicherheitsdatei abgelegt. Die anschließende Frage "Öffentlichen Schlüssel für ... zur Bank übertragen?" bestätigen Sie mit "Ja". Falls Sie den Online-Dialog mit der Bank nicht sofort führen möchten, ist dies auch zu einem späteren Zeitpunkt über den Button "Benutzerdaten aktualisieren" in der Maske "HBCI-Verwaltung" möglich.

Es wird nun eine Online-Verbindung zum Rechenzentrum Ihrer Bank aufgebaut. Während der Übertragung wird der sogenannte Hashwert des öffentlichen Schlüssels der Bank als 40-stellige Buchstaben- und Zahlenreihe angezeigt und es erfolgt die Aufforderung, diesen Wert mit dem Wert auf dem INI-Brief der Ihnen von der Bank ausgehändigt wurde zu vergleichen und bei Gleichheit zu bestätigen. Nach der Bestätigung wird Ihr öffentlicher Schlüssel zur Bank übertragen. Nach erfolgreicher Beendigung der Übertragung meldet das Programm im Übertragungsprotokoll "Öffentlicher Schlüssel wurde entgegengenommen" und "Benutzer noch nicht freigeschaltet". Dann wird automatisch der Kunden-INI-Brief gedruckt. Dieser Brief ist zu unterschreiben und an die Bank per Post zu senden. Die Freischaltung des Benutzers erfolgt durch die Bank, sobald Sie Ihren INI-Brief dort eingereicht haben.

Anschließend (in der Regel am nächsten Werktag), können Sie Datenübertragungen unter Nutzung des HBCI-Verfahrens durchführen.

3.d) Sicherheitsprofilwechsel

Wenn Sie bereits mit einer freigeschalteten Sicherheitsdatei mit der Schlüssellänge von 768 Bit arbeiten (Sicherheitsprofil RDH-1), können Sie einen Sicherheitsprofilwechsel auf eine größere Schlüssellänge (Sicherheitsprofil RDH-2) durchführen. Voraussetzung ist, dass Ihre Bank bereits HBCI in der Version 3.0 anbietet und den Sicherheitsprofilwechsel unterstützt. Ist dies der Fall, können über die Funktion "Sicherheitsprofilwechsel" in der HBCI-Verwaltung längere Schlüssel generiert und zur Bank übertragen werden ohne dass eine erneute Freischaltung mit INI-Brief erforderlich ist.

4. HBCI Chipkarte

Zum Lesen und Schreiben von Chipkarten muss ein Chipkartenlesegerät an Ihrem PC angeschlossen und korrekt installiert sein.

Auf der VR-NetWorld-Card (Schlüssellänge 768 Bit) bzw. VR-NetWorld-Card SECCOS (Schlüssellänge 1024-2048 Bit), die bundesweit bei nahezu allen genossenschaftlichen Banken zum Einsatz kommen, sind alle HBCI relevanten Daten (Typ der Chipkarte, Benutzerkennung, Bankleitzahl, Kundennummer/-ID und TCP/IP Adresse) gespeichert. Diese können über die Taste "Chipkartendaten lesen" in das Programm eingelesen werden. Bei der Anlage eines solchen HBCI Benutzers werden Sie nach dem HBCI-Kürzel gefragt. Tragen Sie ein beliebiges HBCI-Kürzel ein, unter dem das Programm den HBCI-Zugang in Zukunft identifiziert. Mit dem auf diese Art angelegten HBCI Benutzer können Sie sofort arbeiten, eine Freischaltung der HBCI Benutzerkennung durch die Bank ist nicht mehr nötig. Die zur Nutzung der VR-NetWorld-Card benötigte PIN wird Ihnen vom Kreditinstitut mitgeteilt und kann nicht geändert werden. Die Karten vom Typ VR-NetWorld-Card SECCOS sind bei Auslieferung mit einer so genannten Karten-Transport-PIN, die Ihnen ebenfalls mitgeteilt wird, gesichert. Beim erstmaligen Einlesen der Karte werden Sie aufgefordert, diese 5-stellige Transport-PIN in eine 6-stellige individuelle PIN zu ändern.

Beim Einlesen von Sparkassen-Chipkarten müssen u. U. noch kundenindividuelle Daten ergänzt werden. Dabei ist darauf zu achten, dass das Feld "Kundennummer/-ID" leer bleibt. Karten vom Typ VR-NetWorld-Card basic (Schlüssellänge 768 Bit) bzw. VR-NetWorld-Card 2 basic (Schlüssellänge 1024-2048 Bit) sowie die von vielen Privatbanken eingesetzten BDB-RSA Karten enthalten bei Auslieferung in der Regel noch keine individuellen Kundendaten. Analog zur Vorgehensweise bei der Sicherheitsdatei werden die von der Bank zur Verfügung gestellten HBCI-Zugangsdaten (Bankleitzahl, Benutzerkennung, Kunden-ID und TCP/IP Adresse) zunächst in der "HBCI Verwaltung" erfasst.

Als Sicherheitsmedium/-verfahren ist "Chipkarte" auszuwählen. Nach dem Speichern der Daten sind diese über die Funktion "Chipkartendaten schreiben" auf die Karte zu schreiben. Handelt es sich um eine neue Karte, werden Sie u. U. aufgefordert eine individuelle PIN zu vergeben bzw. die 5-stellige Transport-PIN in eine 6-stellige individuelle PIN zu ändern. Anschließend werden bei Karten vom Typ VR-NetWorld-Card basic analog zum Verfahren mit Sicherheitsdatei die Sicherheitsschlüssel auf die Karte generiert. Bei Karten vom Typ VR-NetWorld-Card 2 basic befinden sich die Schlüssel bereits auf der Karte. Nach der Initialisierung beim Kreditinstitut (z.B. über die Funktion "Benutzerdaten aktualisieren") wird der Kunden-INI-Brief ausgedruckt, der dem Kreditinstitut auszuhändigen ist. Ist dort die Freischaltung erfolgt, kann mit der Karte gearbeitet werden.

5. PIN/TAN-Interface (PIN / TAN über HBCI/FINTS)

Das PIN/TAN-Interface bedient sich einer SSL-gesicherten Datenübertragung im Internet auf Basis des HBCI-Protokolls. Die Legitimation des Benutzers geschieht analog zum Internetbanking mittels PIN und TAN.

Aus der "HBCI-Verwaltung" gelangen Sie über die Taste "Neu..." oder "Bearbeiten..." zur manuellen Anlage neuer HBCI-Benutzer. Tragen Sie hier ein beliebiges HBCI-Kürzel ein, unter dem das Programm den HBCI-Zugang in Zukunft identifiziert.

Unter Sicherheitsmedium/-verfahren wählen Sie "PIN / TAN".

Die weiteren Zugangsdaten wurden Ihnen von Ihrer Bank mitgeteilt. Für genossenschaftliche Institute (Volks- und Raiffeisenbanken) im norddeutschen Raum (GAD-Banken, GLS Bank) sind dies Ihre Kundennummer und die Kontonummer. Bei genossenschaftlichen Instituten im Süden und Osten Deutschlands (Fiducia-Banken) ist der sogenannte VR-NetKey einzugeben. Bei den Sparkassen ist entweder die Kontonummer oder ein Anmeldenname (auch Zugangsbenutzerkennung) einzugeben.

Die Speicherung der PIN bei den HBCI-Parametern ist optional, da dies u. U. ein Sicherheitsrisiko darstellen kann. Wird die PIN nicht abgespeichert, so wird sie vor jeder Datenübertragung abgefragt.

Unter "Internet-Adresse" tragen Sie bitte, sofern sie nicht automatisch vorgeschlagen wird, die HBCI-Internet-Adresse ein, die Ihnen ebenfalls von Ihrer Bank mitgeteilt wurde. Achten Sie dabei auf die exakte Schreibweise einschließlich der Groß- und Kleinschreibung!

Nach dem Speichern dieser Daten können direkt HBCI-Geschäftsvorfälle ausgeführt werden. Sofern eine Legitimation mittels TAN erforderlich ist, wird diese während der Datenübertragung abgefragt.

Falls im Profi cash Datenbestand noch Konten zu diesem HBCI Zugang gefunden werden, die bereits für einen BTX-Zugang konfiguriert waren, werden diese automatisch auf das PIN/TAN-Interface Verfahren umgestellt. Auch bereits angelegte Umsatzabfragejobs werden an das neue Verfahren angepasst.

Unterstützt Ihre Bank neben dem klassischen PIN/TAN Einschrittverfahren auch ein sogenanntes Zweischrittverfahren (z.B. iTAN, mTAN oder Sm@rt-TAN plus) so wird Ihnen dies beim nächsten Onlinedialog mit der Bank mitgeteilt. Sofern mehrere Verfahren angeboten werden, haben sie die Möglichkeit eines der Verfahren für die zukünftige Nutzung auszuwählen. Wird nur ein Verfahren angeboten, wird dieses automatisch eingestellt und Sie werden darüber informiert. Das Verfahren kann auch noch nachträglich unter "HBCI-Verwaltung / Bearbeiten... / TAN-Verfahren..." geändert werden.

Der Unterschied zum klassischen Einschrittverfahren besteht darin, dass Sie zur Freigabe von Aufträgen nicht mehr eine beliebige TAN verwenden dürfen. Während der Datenübertragung wird Ihnen mitgeteilt, wie die TAN zu ermitteln ist (z.B. bei Sm@rt-TAN plus), bzw. welche TAN aus dem TAN-Bogen zu verwenden ist (z.B. bei iTAN).

6. Kontenanlage

Sofern Sie unter " Stammdaten - Konten Auftraggeber" bereits manuell Konten erfasst haben, tragen Sie das soeben angelegte HBCI-Kürzel bei dem zugehörigen Konto ein und speichern die Daten, um diese Konten HBCI-fähig zu machen.

Noch nicht in Profi cash vorhandene Konten, für die Sie berechtigt sind, werden automatisch angelegt, sobald Sie erstmalig eine HBCI-Verbindung zur Bank aufbauen (z.B. über den Knopf "Benutzerdaten aktualisieren" in der HBCI-Verwaltung).

In sogenannten UPD-Dateien (User-Parameter-Dateien) stellt Ihnen die Bank Informationen darüber zur Verfügung, auf welche Konten Sie mit diesem HBCI-Kürzel zugreifen können. Diese UPD-Dateien werden vom Programm ausgewertet und die darin enthaltenen Konten werden, sofern noch nicht vorhanden, angelegt. Gleichzeitig wird für jedes neue Konto ein Umsatzabfragejob angelegt.

7. Statusprotokoll holen

Je nach Kreditinstitut und Umfang der übertragenen Daten werden Zahlungsverkehrsaufträge nicht immer direkt als verarbeitet oder fehlerhaft quittiert, sondern u. U. vom Rechenzentrum zunächst nur entgegengenommen. Dies wird Ihnen entsprechend mitgeteilt. In diesem Fall ist es notwendig, kurze Zeit später unter "HBCI-Verwaltung - Statusprotokoll holen" zu der entsprechenden Benutzerkennung bzw. HBCI-Kürzel das aktuelle Statusprotokoll abzuholen und sich vom Verarbeitungszustand der Aufträge zu überzeugen. Alternativ kann unter dem Menüpunkt "Tagesgeschäft - Joberstellung - Statusprotokoll über HBCI" ein Job zum regelmäßigen Abholen des Statusprotokolls angelegt werden.

Zahlungsverkehrsjobs, welche nur entgegengenommen wurden, bleiben nach der Übertragung in der Übersicht unter dem Menüpunkt "Tagesgeschäft - HBCI unterschreiben" stehen und werden nach 15 Tagen automatisch gelöscht bzw. können über die Funktion "Widerrufen" wieder aktiviert werden.

Bei allen Fragen zum Online-Banking erreichen Sie uns unter der Rufnummer 0234 / 5797 444.

GLS Bank, Postfach 10 08 29, 44708 Bochum
kundenberatung@gls.de
www.gls.de

Telefonische Kundenberatung: 0234 / 5797 111