firm

Kundenleitfaden
Einrichtung HBCI

Finanzen. Professionell. Managen.

Februar 2018

Inhalt

Copyrights und Warenzeichen

1 HBCI mit PIN und TAN einrichten

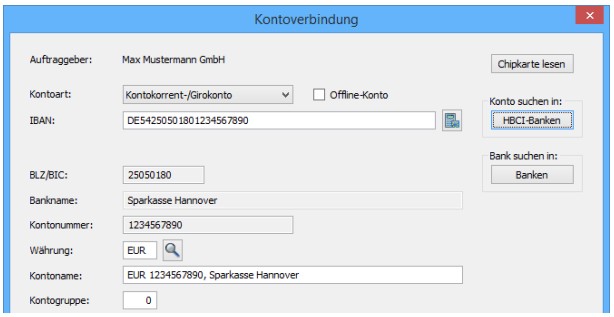
Um einen Datentransfer per HBCI (Homebanking Computer Interface) durchführen zu können, muss die Kontoverbindung zunächst für diesen Übertragungsweg konfiguriert werden. Die derzeit von SFirm unterstützten HBCI-Verfahrensweisen sind die per *PIN/TAN*, per *Sicherheitsdatei* und per Chipkarte.

In diesem Kapitel wird die Einrichtung von HBCI PIN/TAN innerhalb von SFirm beschrieben. Ein Großteil der Konfiguration ist für alle Varianten des HBCI PIN/TAN-Verfahrens gleich. Auf abweichende Schritte oder Besonderheiten in der Einrichtung wird an entsprechender Stelle hingewiesen.

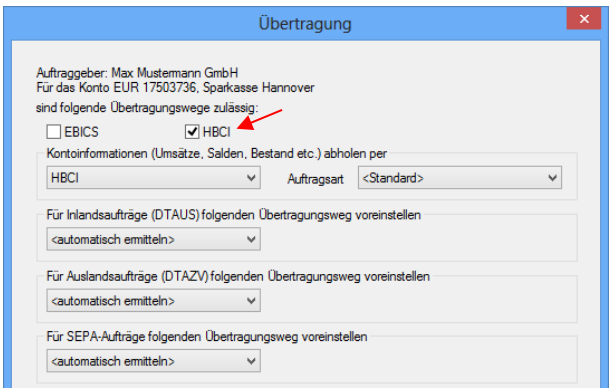
Die Konfiguration des Übertragungsweges für HBCI mit PIN/TAN wird hier vorausgesetzt.

1.1 Einstieg in die Einrichtung

Die Neuanlage eines Kontos wird im Reiter *Kontoverbindung* vorgenommen. Hinterlegen Sie dort zunächst die Stammdaten zu der Kontoverbindung.



In der Übertragung wählen Sie nun das Verfahren *HBCI* aus. Bei Bedarf können noch weitere Wege definiert werden, was aber vorzugsweise nacheinander geschehen sollte. Das Abholen der Kontoumsätze mit HBCI wird automatisch vorbelegt. Mit den <Weiter>-Schaltflächen werden nun weitere Dialoge angezeigt.

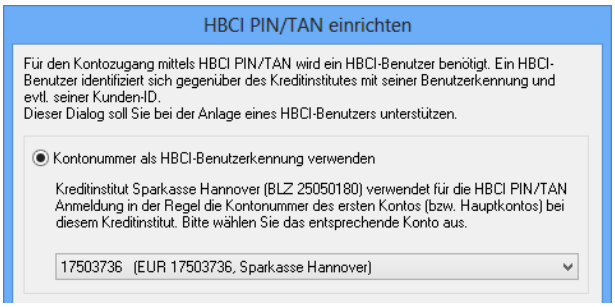


Zu diesen gehören - je nach lizenzierten Modulen - die Dialoge *Cash*, *Depooling*, *AZV*, *MT101*, *HBCI*, und *Rundrufdefinition*.

1.2 Assistent zur Einrichtung ausführen

Kurz vor dem Abschluss der Kontoeinrichtung erscheint automatisch der Dialog *HBCI einrichten*, der Assistent für die Konfiguration von HBCI. Wählen Sie *HBCI mit PIN und TAN* aus und bestätigen Sie die Auswahl mit <OK>.

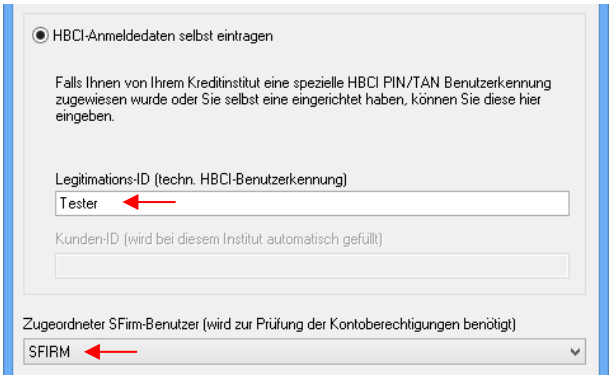
Die Anmeldung am Bankrechner erfolgt häufig mit der Kontonummer des ersten bzw. des Hauptkontos. Wenn die Angaben für HBCI aus der Kontonummer abgeleitet werden können, markieren Sie den Parameter *Kontonummer als HBCI-Benutzerkennung verwenden*. Wählen Sie aus der Liste das entsprechende Konto aus.



Bei den Verfahren…

- chipTAN
- SmartTAN
- smsTAN
- pushTAN
- photoTAN

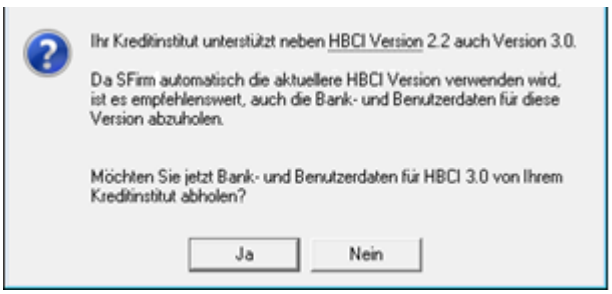
muss hier i.d.R. die Legitimations-ID hinterlegt werden. Je nach ausgewähltem Institut ist eine zusätzliche Eingabe der Kunden-ID erforderlich.



Beachten Sie bitte, dass bei vielen Sparkasse vor der Nutzung von chipTAN (vor allem wenn von einem anderen Verfahren auf chipTAN gewechselt wurde) das chipTAN-Verfahren über das Internet-Banking vom Kunden freigeschaltet werden muss.

Legen Sie anschließend den zugeordneten SFirm-Benutzer fest und schließen Sie die Eingaben mit <OK> ab. SFirm möchte daraufhin Kontakt zum Kreditinstitut aufnehmen, um den Zugang zu synchronisieren. Bestätigen Sie dies mit <OK> und Authentisieren Sie im darauffolgenden Schritt diesen Transfer mit Ihrer PIN.

Evtl. erhalten Sie nebenstehende Meldung, dass das Kreditinstitut neben der HBCI-Version 2.2 auch die Version 3.0 unterstützt. Liegen Ihnen keine abweichenden Informationen vor, können Sie die Synchronisation des Zugangs für HBCI 3.0 mit <Ja> bestätigen.



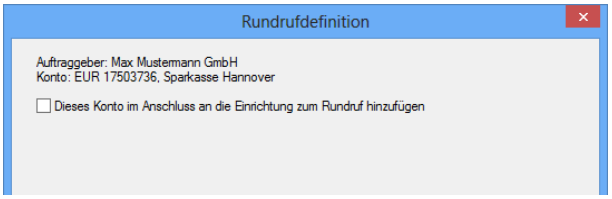
1.3 Verfügungsberechtigte / Rundrufdefinition

Nach dem die Daten erfolgreich transferiert wurden, erscheint eine Abfrage, ob für dieses Konto weitere HBCI-Benutzer eingerichtet werden sollen.

Wurde die Frage mit <Ja> beantwortet, wird erneut eine Verbindung zum Institut hergestellt um die aktuellen HBCI PIN/TAN Benutzerdaten für den zweiten Benutzer abzuholen.

Anschließend erscheint die Meldung, dass die Einrichtung des Übertragungsweges *HBCI PIN/TAN* abgeschlossen ist.

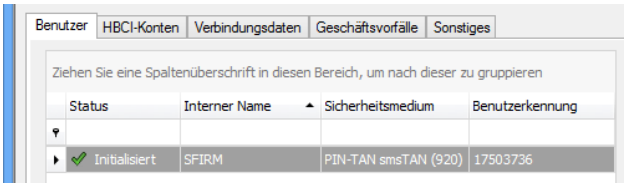
Daraufhin (und wenn die Frage nach einem weiteren Verfügungsberechtigten verneint wurde), der Dialog *Rundruf-definition angezeigt*. In diesem Dialog können Sie wählen, ob das Konto im Anschluss zum Rundruf hinzugefügt werden soll.



Nach Bestätigung der Schaltfläche <Fertig stellen> ist die Kontoanlage abgeschlossen. Sollten mit der Synchronisation des Zugangs weitere Konten neben dem bereits in SFirm hinterlegten vorhanden sein, können Sie mit der Anlage dieser Konten jetzt fortfahren. Die weiteren Schritte, die je nach Beantwortung dieser Hinweismeldung folgen, werden in dem Abschnitt Weitere Konten des gleichen Instituts einbinden beschrieben. Abschließend sehen Sie (wie zu Beginn der Einrichtung) den Dialog *Bankverbindung ändern* mit dem Reiter *Übertragung* zur abschließenden Kontrolle angezeigt.

Das Verfahren des Benutzers wird in jedem Fall nach der Dialoginitialisierung ein- bzw. umgestellt. Sollte das Verfahren von SFirm nicht unterstützt werden, erhalten Sie bei der Übertragung von Aufträgen eine entsprechende Rückmeldung im HBCI Protokoll.

Über *Stammdaten ▸ Bankzugänge ▸ HBCI ▸ HBCI-Bankzugang* wird Ihnen im Reiter *Benutzer* der neue HBCI-Benutzer mit dem entsprechende Sicherheitsmedium und der Benutzerkennung angezeigt.



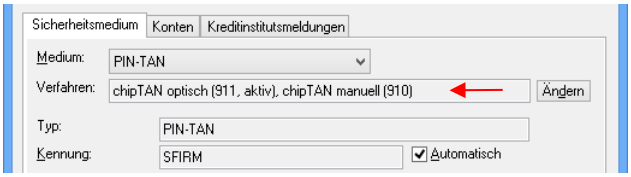
1.4 Weitere Verfahren bzw. Wechsel zwischen den TAN-Verfahren

Soll die Einrichtung von HBCI PIN/TAN für die Verfahren…

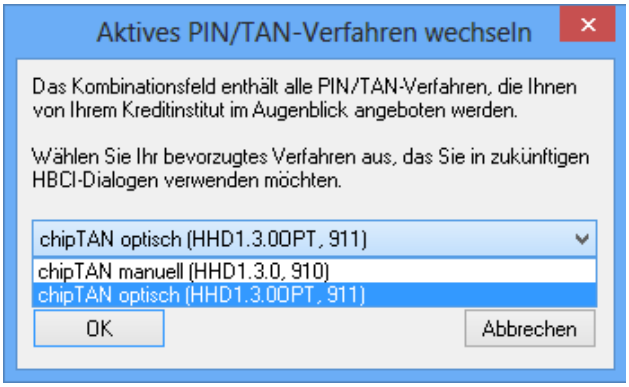
- chipTAN
- SmartTAN
- smsTAN
- pushTAN
- photoTAN

vorgenommen werden, markieren Sie im Reiter *Benutzer* den neue HBCI-Benutzer und klicken Sie auf die Schaltfläche <Ändern>.

Damit gelangen Sie in den Dialog *Benutzer bearbeiten*. Sie sehen in dem Feld *Verfahren:* das momentan hinterlegte Verfahren angezeigt.



Klicken Sie nun auf die Schaltfläche <Ändern> hinter dem Feld *Verfahren:* Damit öffnet sich der Dialog *Aktives PIN/TAN-Verfahren wechseln*. Wechseln Sie hier auf das entsprechende Verfahren und bestätigen Sie die Auswahl mit <OK>.



Dies ist grundsätzlich die Vorgehensweise für den Wechsel eines TAN-Verfahrens. Liegt das neue Verfahren SFirm noch nicht vor, müssen zunächst die verfügbaren Verfahren über *Zugang synchronisieren* aktualisiert werden. Wird das neue Verfahren anschließend immer noch nicht aufgeführt, ist es i.d.R. bankseitig noch nicht freigeschaltet.

Die Einrichtung der Verfahren…

- iTAN
- smsTAN
- pushTAN
- photoTAN

ist damit abgeschlossen. Zum Abschluss der Verfahren…

- chipTAN
- SmartTAN

folgen im nächsten Abschnitt weitere Informationen. Die Einrichtung des Verfahrens smsTAN wird mit den Schritten des übernächsten Abschnitts abgeschlossen.

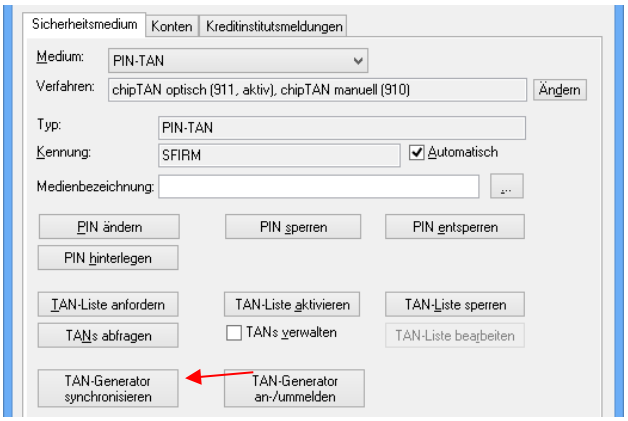
1.4.1 chipTAN (optisch/manuell)

1.4.1.1 TAN-Generator synchronisieren

Vor der erstmaligen Verwendung des HBCI-Verfahrens sollte bei den Verfahren…

- chipTAN
- SmartTAN

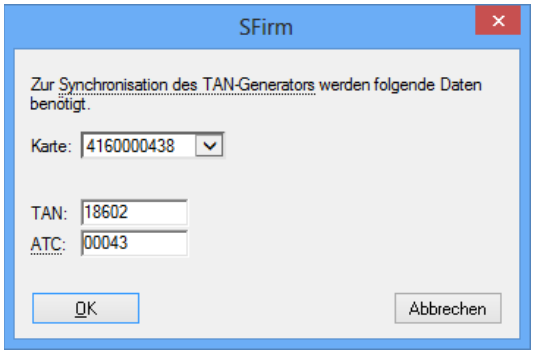
der TAN-Generator synchronisiert werden (Schaltfläche *TAN-Generator synchronisieren*).



Bei dem genannten Verfahren wird die TAN mit Hilfe des TAN-Generators und einer eingelegten Chipkarte errechnet. Jede TAN erhält dabei eine laufende Nummer, die als *ATC* bezeichnet wird. Bankseitig existiert ebenfalls ein ATC für Ihre Chipkarte, die Ihnen i.d.R. aber nicht Online angezeigt wird. Jedes Mal, wenn Sie mit Ihrer Chipkarte und dem TAN-Generator eine TAN generieren, erhöht sich der ATC Ihrer Karte um eins. Wird diese TAN im Online-Banking verwendet, erhöht sich der zugehörige, bankseitige ATC Ihrer Karte ebenfalls um eins. Verwenden Sie die erzeugte TAN allerdings nicht, erhöht sich nur der ATC auf Ihrer Karte und es entsteht eine Differenz zum bankseitigen ATC. Wenn diese Differenz größer als 25 ist, wird die von Ihnen erzeugte TAN vom Online-Banking-System aus Sicherheitsgründen abgelehnt. In diesem Fall ist eine Synchronisation des ATC Ihrer Karte mit dem bankseitigen ACT notwendig.

Über die Schaltfläche <TAN-Generator synchronisieren> haben Sie die Möglichkeit diese Synchronisation vorzunehmen. Geben Sie zunächst in dem Feld Kartennummer die Kartennummer der verwendeten Chipkarte ein. Alternativ können Sie über den Link *Verfügbare Karten ermitteln* SFirm anweisen, die verfügbaren Karten online bei Ihrem Institut zu erfragen.

Liegen mehrere Karten vor, können Sie die entsprechende anschließend über das Auswahlfeld selektieren (haben Sie die Kartennummer manuell eingegeben, steht dieses Auswahlfeld nicht zur Verfügung). Ermitteln Sie anschließend die ATC der Chipkarte über den TAN-Generator.



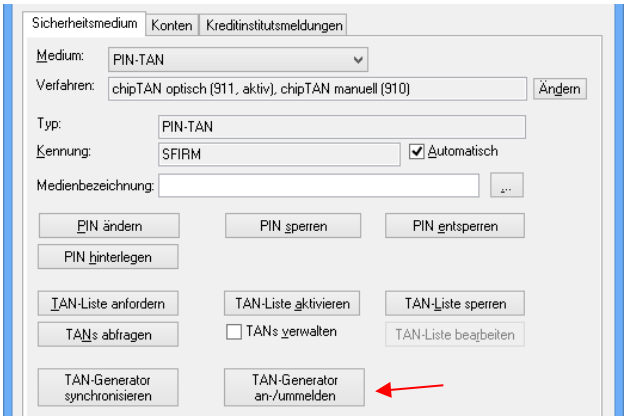
Wie Sie den aktuellen ATC Ihrer Chipkarte über den TAN-Generator in Erfahrung bringen, entnehmen Sie bitte der Dokumentation des Gerätes. Bei dem Gerät *tan-Jack optic* von *REINER-SCT* ist das Vorgehen dazu laut Anleitung wie folgt:

„Halten Sie bei eingeführter Chipkarte die TAN-Taste so lange gedrückt, bis „ATC Anzeige aktiviert“ im Display erscheint. Drücken Sie danach einmal die TAN-Taste. Es wird Ihnen nun neben der TAN auch der ATC angezeigt.“

Im Display des TAN-Generators sollte schließlich der ATC und eine TAN angezeigt werden. Geben Sie beide Werte in die entsprechenden Felder ein und bestätigen Sie die Eingabe mit <OK>. Anschließend erhalten Sie die Erfolgsmeldung *„TAN Generator Synchronisierung“ erfolgreich durchgeführt*.

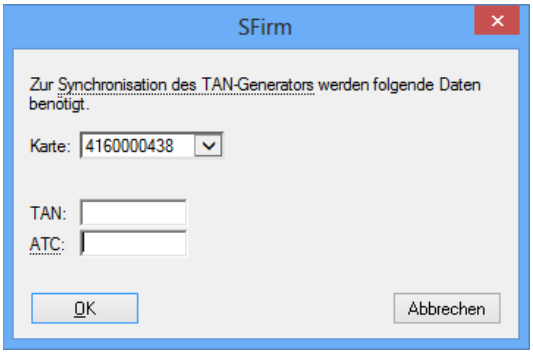
1.4.1.2 TAN-Generator an-/ummelden

Wenn Sie TAN pflichtige Aufträge ausführen, muss bei Annäherung bzw. Überschreitung des Verfallsdatums Ihrer ec-Karte mit chipTAN-Funktion eine Freischaltung/Ummeldung Ihrer neuen Karte, bzw. des TAN-Generators erfolgen.



Über die Schaltfläche <TAN-Generator an-/ummelden> haben Sie die Möglichkeit diese Ummeldung vorzunehmen. Geben Sie zunächst in dem Feld Kartennummer die Kartennummer der verwendeten Chipkarte ein. Alternativ können Sie über den Link *Verfügbare Karten ermitteln* SFirm anweisen, die verfügbaren Karten online bei Ihrem Institut zu erfragen.

Liegen mehrere Karten vor, können Sie die entsprechende anschließend über das Auswahlfeld selektieren (haben Sie die Kartennummer manuell eingegeben, steht dieses Auswahlfeld nicht zur Verfügung). Ermitteln Sie anschließend die ATC der Chipkarte über den TAN-Generator.



Werden die Eingabefelder *TAN* und *ATC* nicht angezeigt, sind diese Angaben für die Ummeldung bei diesem Institut nicht notwendig.

1.4.2 chipTAN USB

1.4.2.1 Allgemein

Neben den bewährten Verfahren chipTAN optisch und manuell, wurde ein weiterentwickeltes chipTAN-Verfahren in SFirm implementiert.

Bei dem chipTAN USB wird ein USB-Kartenleser eingesetzt, der annähernd die gleiche Funktionalität wie ein kabelloser chipTAN-Leser mitbringt. Die TAN wird allerdings nicht durch einen Flickercode, sondern innerhalb des Kartenlesers erzeugt. Dabei übernimmt SFirm während eines Auftragsversands, automatisch die vom Kartenleser zurückgelieferte TAN.

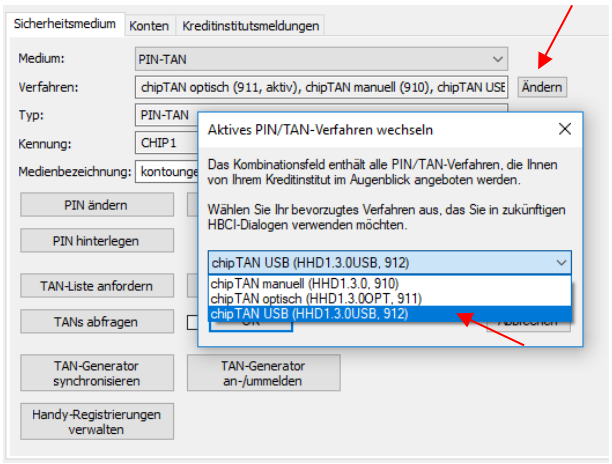
> Wenn Sie bei Ihrem Institut das chipTAN-/SmartTAN-Verfahren bereits nutzen, können Sie das Verfahren ebenfalls als chipTAN USB nutzen, sobald ein entsprechender Kartenleser angeschlossen ist.

Wenn Sie von Ihrem Institut für das Verfahren freigeschaltet wurden, muss dieses In SFirm noch hinterlegt und konfiguriert werden.

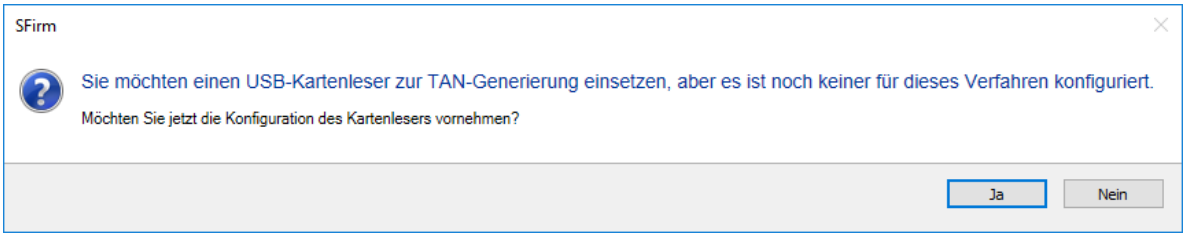
1.4.2.2 Verfahren wählen

Um das Verfahren zu nutzen, synchronisieren Sie zunächst den Bankzugang.

Öffnen Sie anschließend bitte den HBCI-Benutzer und klicken neben der Spalte *Verfahren* auf <Ändern>. Zur Auswahl sollte neben den bisherigen chipTAN-Verfahren das chipTAN USB zur Verfügung stehen. Wählen Sie es bitte aus und bestätigen die Auswahl mit <OK>

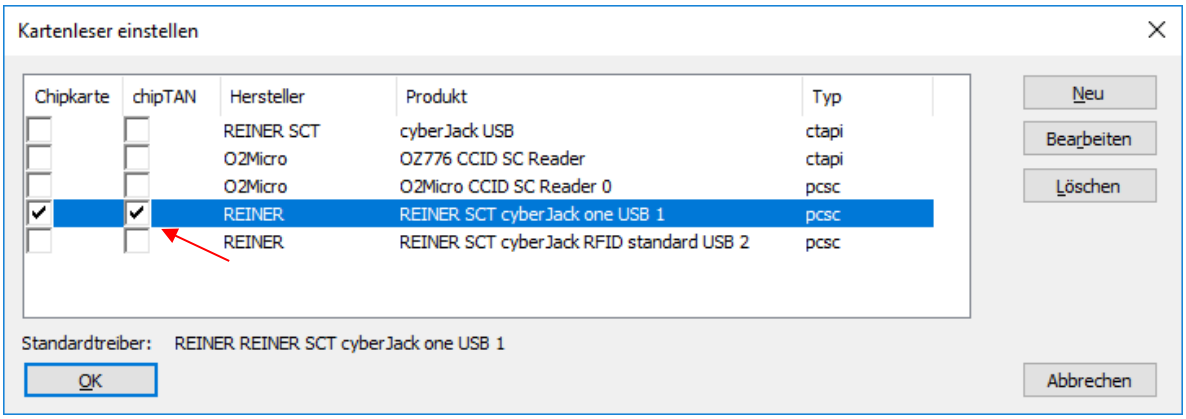


Anschließend prüft SFirm, ob ein geeigneter Kartenleser angeschlossen und verfügbar ist. Wenn das nicht der Fall sein sollte, erscheint die folgende Meldung:



Wenn Sie diese mit <Ja> bestätigen, öffnet sich der Einstellungsdialog der Kartenleser in SFirm:

1.4.2.3 Kartenleser einstellen



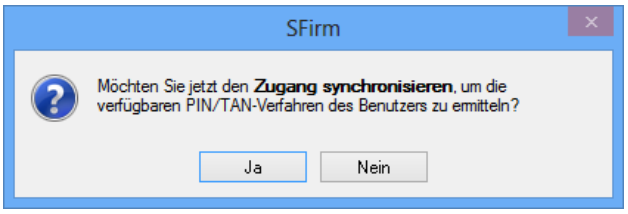
In dem hier abgebildeten Beispiel handelt es sich um einen **REINER SCT cyber jack one** USB-Kartenleser. Da dieser Kartenleser beide Verfahren unterstützt, kann er für beide aktiviert werden. Wenn Sie für die bisherigen Verfahren allerdings noch weiterhin Ihren bisherigen Kartenleser nutzen möchten, ist es ebenfalls problemlos möglich.

Eine Unterstützung von Bluetooth-Kartenlesern ist momentan nicht vorgesehen.

Bestätigen Sie den Kartenleser-Dialog mit <OK>. Die Einrichtung des Verfahrens ist damit abgeschlossen. Sollten Sie während einer Übertragung dazu aufgefordert werden, den TAN-Generator zu synchronisieren, beachten Sie bitte die die Kapitel TAN-Generator synchronisieren. Wenn Sie eine neue oder eine andere Karte einsetzen möchten folgen Sie bitte der Beschreibung unter TAN-Generator an-/ummelden.

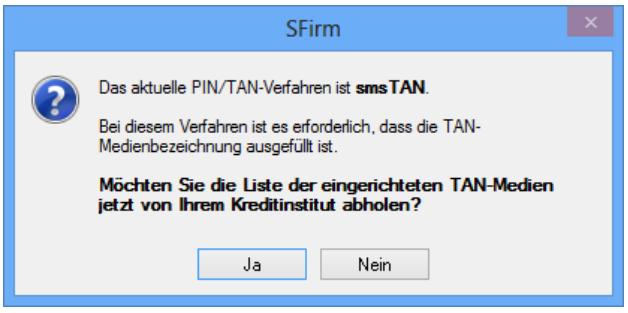
1.4.3 smsTAN/pushTAN

Für das Anlegen eines HBCI-Benutzers, der für das sms-TAN/pushTAN freigeschaltet ist geben Sie die entsprechenden Benutzerdaten ein und klicken im Einrichtungsdialog auf <OK>. Anschließend erhalten Sie die nebenstehende Meldung.

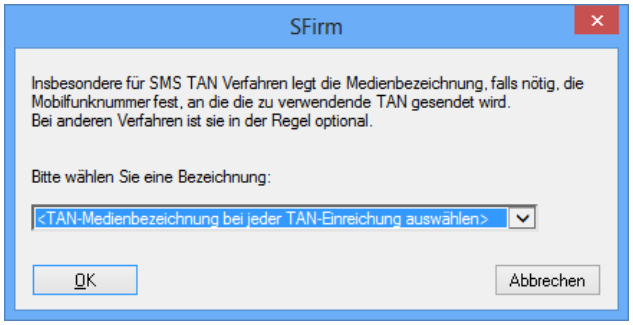


Bestätigen Sie diese bitte mit <Ja>.

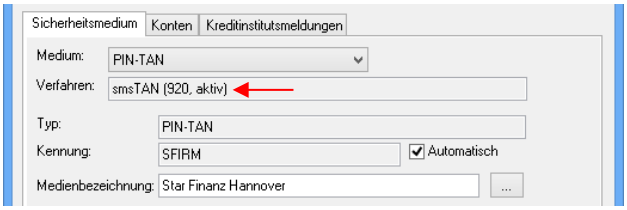
Nachdem der Kontakt zum Institut stattgefunden hat, erhalten Sie nun die nebenstehende Meldung, dass für dieses Verfahren die sog. Medienbezeichnungen angefordert bzw. ausgefüllt werden müssen. Bestätigen Sie dies mit <Ja> und Authentisieren Sie im zweiten Schritt den Transfer mit Ihrer PIN.



Nur wenn mehrere TAN-Medien vorliegen, erhalten Sie nebenstehende Meldung. Wählen Sie hier die zu verwendende Bezeichnung aus und bestätigen Sie die Auswahl mit <OK>.

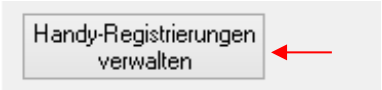


Eine Kontrolle des gewählten Verfahrens ist über den Reiter *Sicherheitsmedium*, im Feld *Verfahren:* möglich. Die Einrichtung von smsTAN ist damit abgeschlossen.



1.4.3.1 Handy-Registrierungen verwalten (smsTAN)

Hier haben Sie die Möglichkeit, Handy-Registrierungen zu verwalten. Nach der Eingabe Ihrer PIN werden die hinterlegten Registrierungen vom Kreditinstitut abgeholt.



In der Übersicht werden die registrierten Mobiltelefone angezeigt.

Hier können Sie die registrierten Mobiltelefone ändern, deaktivieren und löschen.

Zusätzlich können Sie hier eine erstmalige Handy-Handy-Registrierung durchführen oder zusätzliche Mobiltelefone registrieren.

Mobilfunkverbindung registrieren

Mit der Funktion <Neue Handy-Registrierung> kann eine neue oder zusätzliche Mobilfunkbezeichnung hinterlegt werden.

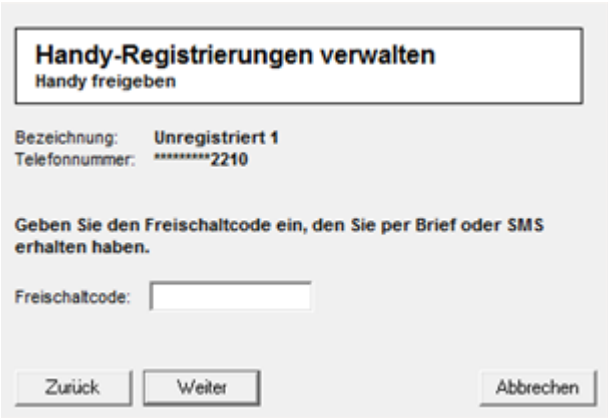
Nach der Eingabe der Bezeichnung und der dazugehörigen Telefonnummer, erfolgt ein Dialog in dessen Verlauf Sie nach einer TAN gefragt werden, die Ihnen auf das in SFirm aktuell hinterlegte Handy (bei zusätzlicher Registrierung) geschickt wird.

Nach der Eingabe der TAN wird die neue Telefonnummer registriert.

Sollte es sich um die erstmalige Handy-Registrierung handeln, wird Ihnen ein Freischaltcode per Post zugeschickt.

Mobilfunkverbindung freischalten

Sollte bei einer Telefonnummer die Aktion <Freigeben> erscheinen, ist das Handy bei Kreditinstitut zwar registriert, für die Nutzung mit smsTAN jedoch noch nicht freigegeben. Beim Aufruf wird ein Freischaltcode abgefragt, welcher Ihnen per Brief oder SMS mitgeteilt wurde.



Nach dessen Eingabe wird das Telefon für die Nutzung des smsTAN freigegeben.

Mobilfunkverbindung ändern

Mit der Funktion <Ändern> kann die Bezeichnung des Handys und die hinterlegte Telefonnummer geändert werden.

An dieser Stelle müssen nicht zwingend beide Angaben geändert werden. Wenn Sie nur die Bezeichnung des Telefons ändern möchten, lassen Sie das Feld *Telefonnummer* frei.

Mobilfunkverbindung deaktivieren/löschen

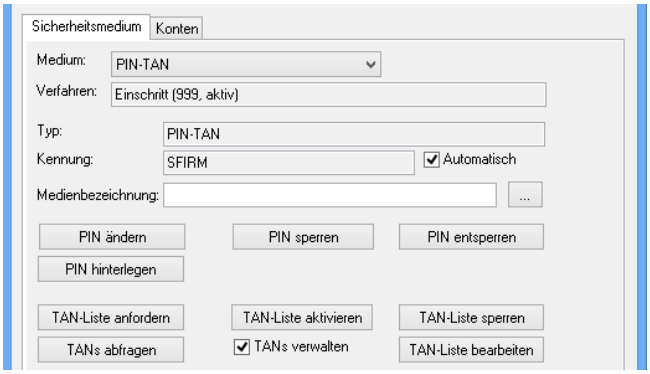
Mit der Funktion <Deaktivieren> bzw. <Löschen> kann das Handy als Medium temporär deaktiviert oder gelöscht werden.

1.5 Verfahrensübergreifende Einstellungen

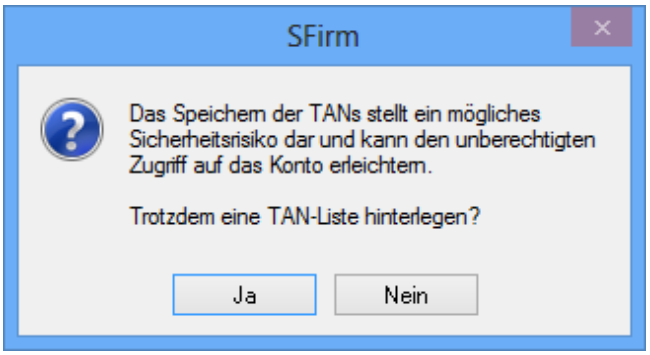
1.5.1 TAN-Liste verwalten

Grundsätzlich kann die Verwaltung einer TAN-Liste auch von SFirm übernommen werden. Aus Sicherheitsgründen wird aber davon abgeraten, diese Möglichkeit zu nutzen.

Rufen Sie beim Auftraggeberkonto im Reiter *HBCI* den betreffenden Benutzer auf. Markieren Sie den Benutzer und klicken Sie auf <Ändern>.

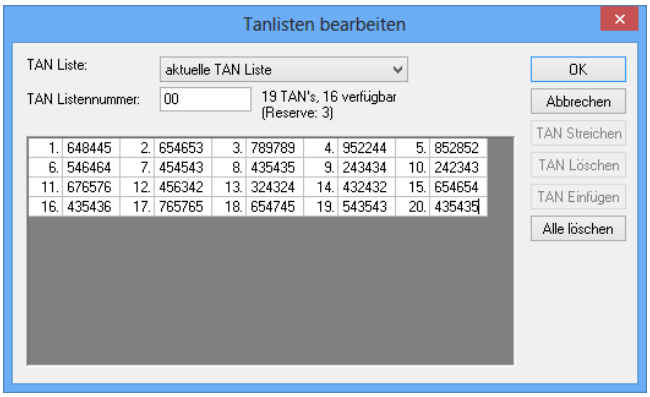


Setzen Sie hier bitte den Haken bei *TANs verwalten*. Daraufhin werden Sie darauf hingewiesen, dass das Speichern der TAN-Liste ein evtl. Sicherheitsrisiko birgt. Bestätigen Sie dies mit <Ja>.



Nach dem Sie die PIN eingegeben haben, haben Sie die Möglichkeit mit *TAN-Liste bearbeiten* die TANs zu hinterlegen

Die Erfassung einer TAN-Liste ist bei iTAN um die Spalten für den Index der TAN erweitert. Dieser Index kann nicht verändert werden.



Die Felder des Dialogs *TAN-Listen bearbeiten* im Einzelnen:

TAN Liste	Für HBCI mit PIN und TAN werden bis zu zwei TAN-Listen pro Konto verwaltet. Wenn Sie erstmalig an der elektronischen Kontoführung teilnehmen, wählen Sie die Einstellung *Aktuelle TAN-Liste* aus.

TAN Listennummer	Für die Liste wird die Listennummer - soweit diese vom Institut mitgeteilt wird - eingegeben. Anschließend klicken Sie in das erste Eingabefeld zur Erfassung der TANs.
TAN streichen	Die „gestrichenen TANs“ wurden z. B. bereits für die Übertragung verwendet und können von Ihnen nicht mehr für Transaktionen genutzt werden. Wenn Sie jedoch eine TAN in der Liste erfasst und diese TAN bereits verbraucht haben, müssen Sie die TAN manuell über <TAN Streichen> streichen. Alternativ können Sie die TAN auch löschen.
TAN einfügen	Zum Einfügen einer neuen TAN. Ein Index kann für die einzugebende TAN ebenfalls angeben werden. Mit der Bestätigung der TAB- oder der Enter-Taste wird das nächste Feld zur Erfassung angezeigt. Die erfassten TANs werden erst gespeichert, wenn Sie die Schaltfläche <OK> bestätigen.
TAN löschen	Die Löschung erfolgt, wenn Sie das Feld markieren und die Schaltfläche <TAN löschen> auswählen. Beim nächsten Aufruf wird der entsprechende Eintrag in der Liste nicht mehr aufgeführt.
Alle löschen	Alle TANs der ausgewählten Liste werden unwiderruflich gelöscht.

Wenn Ihnen nur noch wenige TAN-Nummern zur Verfügung stehen, muss bei einigen Instituten eine neue TAN-Liste angefordert werden. Bei anderen Instituten wird nach dem Verbrauch einer bestimmten Anzahl von TANs automatisch eine neue TAN-Liste zugeschickt. Wenn Sie eine neue TAN-Liste angefordert haben bzw. eine neue TAN-Liste vom Institut zugeschickt wurde, jedoch die TANs der aktuellen Liste noch nicht verbraucht sind, können Sie bereits die Nummern der neuen TAN-Liste erfassen. Die neuen Nummern werden unter der Einstellung „Nächste TAN-Liste“ eingegeben. Die TANs der neuen Liste werden erst gültig, wenn Sie diese bei Ihrem Institut aktivieren.

Die TAN-Listen werden dem HBCI-Benutzer (und nicht dem Konto) zugeordnet. Wenn ein Benutzer Unterschriftsberechtigungen für mehrere Konten bei einem Institut hat, gilt die TAN-Liste für mehrere Konten. Umgekehrt gilt, dass bei einer Autorisierung nach dem Vier-Augen-Prinzip jeder Benutzer für das Konto seine eigene TAN-Liste verwaltet.

1.5.2 Aktivierung einer TAN-Liste

Wenn Sie die neue TAN-Liste erfasst haben, wird die Liste erst für Transaktionen gültig, wenn Sie beim Institut eine „Aktivierung“ durchführen. Hierzu rufen Sie den Benutzer unter *HBCI-Bankzugang* auf und wählen die Schaltfläche <TAN-Liste aktivieren> aus.

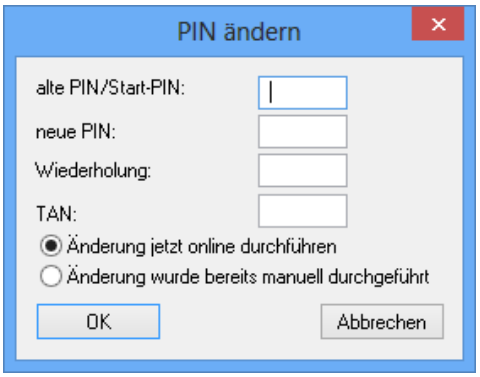
Aktuelle PIN	Geben Sie die Aktuelle PIN für das Konto ein.
TAN aus der alten Liste*	Geben Sie hier eine verfügbare TAN aus der alten Liste ein.
TAN aus der neuen Liste*	Geben Sie hier eine TAN aus der neuen Liste ein.
TAN-Listen-Nummer*	Wenn für das Institut eine TAN-Listen-Nummer vorhanden ist, geben Sie diese für die neue Liste ein.

Änderung jetzt online durchführen	Die Eingabe der Parameter ist nur für Institute möglich, die eine automatische Verarbeitung der Aktivierung auf Institutsseite anbieten. In diesem Fall muss die Änderung sowohl dem Programm als auch dem Kreditinstitut mitgeteilt werden. Die Aktivierung wird im automatischen Dialog durchgeführt.
Änderung wird/wurde bereits manuell durchgeführt	Ist eine Änderung online nicht möglich, wird der Parameter *Änderung wird/wurde bereits manuell durchgeführt* ausgewählt, so dass die neue TAN-Liste als dann aktuelle TAN-Liste im Programm übernommen wird. Ist eine Aktivierung der TAN-Liste auf Institutsseite über das Internet-Banking erforderlich, führen Sie die Aufgaben dort aus.

*Nicht alle Felder werden vom Rechenzentrum zur Aktivierung einer neuen TAN-Liste benötigt. Eingaben können Sie nur in den Eingabefeldern tätigen, die lt. Rechenzentrum zur Aktivierung notwendig sind.

1.5.3 PIN ändern

Wenn Sie die PIN ändern wollen, können Sie dies über diesen Dialog durchführen. Wenn Sie Ihre PIN-Änderung bereits anderweitig Online durchgeführt haben, wählen Sie *Änderung wurde bereits manuell durchgeführt*, um Ihre PIN-Änderung nur in SFirm durchzuführen.



1.5.4 Mehrfachsignaturen

Müssen mehrere Benutzer einen TAN-pflichtigen Auftrag autorisieren, so müssen alle beteiligten Benutzer das gleiche Verfahren (bzw. die gleiche Prozessvariante) verwenden. Wenn Sie mit dem Institut die Autorisierung von Zahlungen nach dem Vier-Augen-Prinzip vereinbart haben, werden für die Benutzerdaten im Reiter *Kontospezifische Daten* der Geschäftsvorfall *Einzelüberweisungen mit „Erstunterschrift (A)* bzw. *Zweitunterschrift (A)* angegeben.

Benutzer mit Zweischrittverfahren und Benutzer mit Einschrittverfahren können einen Auftrag nicht gemeinsam autorisieren.
Es sollte grundsätzlich darauf geachtet werden, dass die Benutzerparameter der beteiligten Benutzer aktuell sind, da immer nur eine Dialoginitialisierung durchgeführt wird und nur Benutzerparameter des dialogführenden Benutzers geliefert werden.

2 HBCI mit Chipkarte einrichten

In diesem Kapitel wird die Verfahrensweise HBCI per Chipkarte behandelt.

2.1 Voraussetzungen zu HBCI mit Chipkarte

Die Voraussetzungen für den Einsatz von SFirm mit HBCI – Chipkarte:

Technische Voraussetzungen / Vorkonfigurationen	Für eine Autorisierung mit Chipkarte müssen ein Chipkartenlesegerät funktionsfähig installiert sein. Eine Beschreibung zur Einbindung von Kartenlesern befindet sich in dem Abschnitt Kartenleser einstellen.
Konfiguration der Übertragungswege	Die Konfiguration des Übertragungsweges für HBCI mit Chipkarte wird hier vorausgesetzt.

Jede Bank, die HBCI anbietet, führt eine Liste von sog. HBCI-Benutzern. Jeder HBCI-Benutzer ist durch eine Benutzerkennung festgelegt, die institutsweit eindeutig ist. Für jeden HBCI-Benutzer ist festgelegt, über welche Konten er mit welchen Berechtigungen verfügen kann.

2.2 HBCI mit einer DDV-Chipkarte konfigurieren

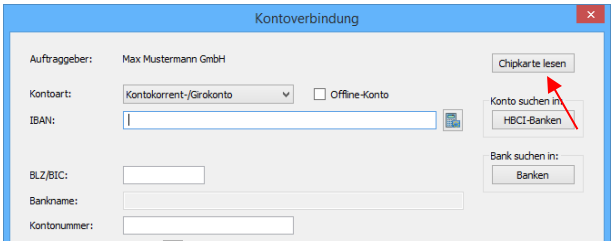
In diesem Abschnitt wird die Einrichtung von HBCI für das Medium Chipkarte beschrieben, zunächst aber ausschließlich für den Chipkarten-Typ DDV (der fast ausschließlich von den Sparkassen/Landesbanken eingesetzt wird). Die Konfiguration eines Kontos für HBCI mit Chipkarte kann – je nach vorliegender Situation – i.d.R. über eine der folgenden Varianten erfolgen:

Neuanlage eines Kontos per HBCI	Die erste Variante betrifft eine Neuanlage eines HBCI-Kontos unter der Hauptgruppe *Stammdaten ▸ Auftraggeber*, bei der auch die Bankverbindung selbst noch nicht in SFirm geführt wird.
HBCI für ein bestehendes Konto einrichten.	Bei der zweiten Variante wird davon ausgegangen, dass bereits ein Konto unter *Stammdaten ▸ Auftraggeber* vorhanden ist und dieses nun dem Übertragungsweg *HBCI* zugeordnet werden soll. Die hier aufgeführte Variante wird in dem Abschnitt HBCI für ein bestehendes Konto einrichten beschrieben.

2.2.1 Neuanlage eines Kontos per HBCI

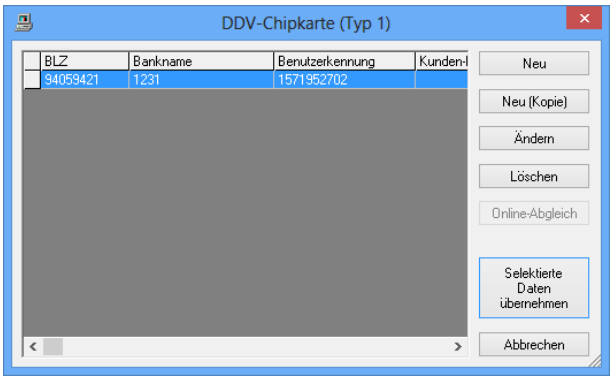
Die hier beschriebene Variante ein Konto für HBCI einzurichten gehört zu der Gängigsten und ist auch die empfohlene. Durch eine strukturierte Abfolge von Dialogen werden das Auftraggeberkonto, der HBCI-Bankzugang, das HBCI-Konto und der HBCI-Teilnehmer „in einem Rutsch“ angelegt. Im Regelfall ist damit keine weitere Konfiguration über verschiedene Programmpunkte und Dialoge notwendig.

Die Einrichtung beginnt über die Schaltfläche <Chipkarte lesen> im Dialog *Kontoverbindung*. Der nebenstehende Dialog erscheint während der Neuanlage eines Auftraggeberkontos.

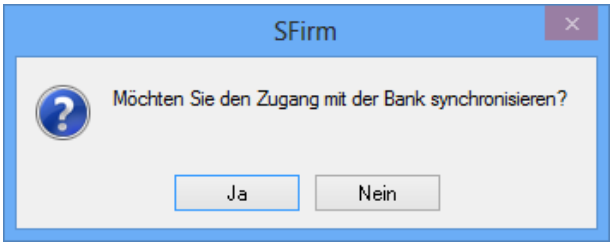


Dieser Dialog kann nachträglich über die Schaltfläche <Neu> bzw. <Ändern> in dem Reiter *Bankkonten* des Dialogs *Auftraggeber* aufgerufen werden.

Die auf der Karte befindlichen und für die Anzeige erforderlichen Daten werden ausgelesen und in dem Fester *DDV-Chipkarte (Typ1)* angezeigt. Sind mehrere Einträge (Zeilen) vorhanden, markieren Sie den gewünschten und klicken Sie anschließend auf die Schaltfläche <Selektierte Daten übernehmen>.



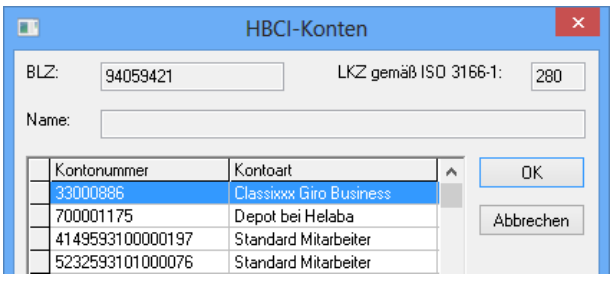
Sie werden anschließend gefragt, ob Sie den Zugang mit der Bank synchronisieren möchten.



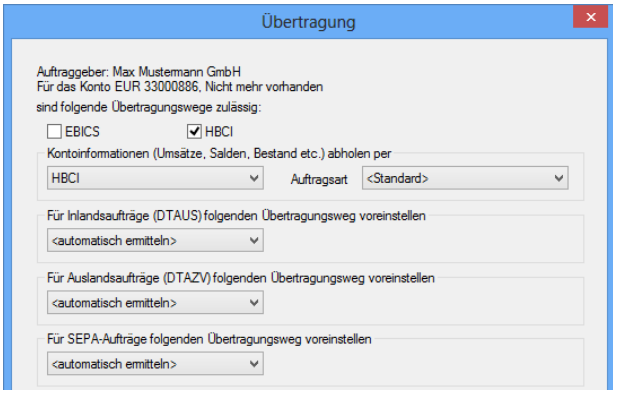
Bestätigen Sie bitte die Meldung mit <Ja>. Die Internetverbindung wird anschließend überprüft und die Dialoginitialisierung durchgeführt.

Zur Authentisierung des Transfers wird die PIN abgefragt. Nach der Eingabe der PIN und der Bestätigung über die Schaltfläche <OK> wird der Zugang mit Ihrem System synchronisiert.

Nach einem erfolgreichen Transfer wird die HBCI-Kommunikation beendet und es erscheint eine Auswahl der verfügbaren Konten des Karteninhabers für dieses Institut in dem Dialog *HBCI Konten*.



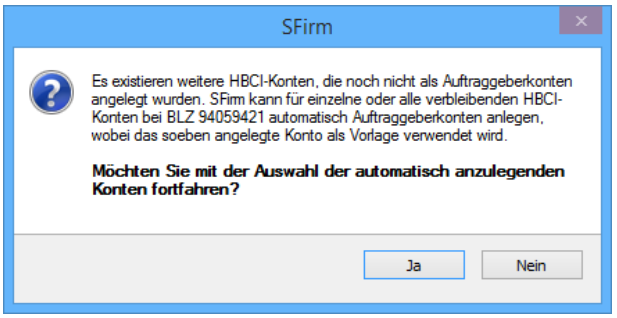
Nach der Selektion eines Kontos und der Bestätigung der Schaltfläche <OK>, erscheint der Dialog *Übertragung*. Der Übertragungsweg *HBCI* wird nun automatisch markiert angezeigt. Ebenso auch die Abholung der Kontoumsätze per HBCI. Automatisch ermittelt wird der Übertragungsweg für den Transfer von DTAUS, DTAZV und SEPA-Aufträgen.



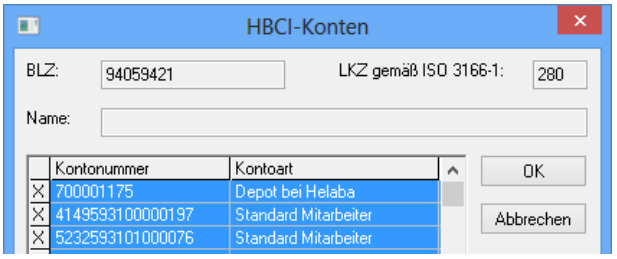
2.2.1.1 Weitere Konten des gleichen Instituts einbinden

Mit den <Weiter>-Schaltflächen werden weitere Dialoge angezeigt. Zu diesen gehören je nach lizenzierten Modulen die Dialoge *Cash*, *Depooling*, *AZV*, *MT101*, *HBCI*, und *Rundrufdefinition*. Nach Bestätigung der Schaltfläche <Fertig stellen> ist die Kontoanlage abgeschlossen.

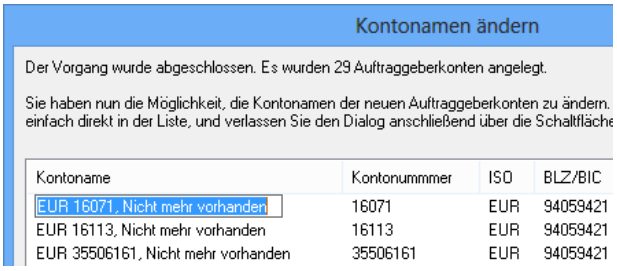
Sollten mit Synchronisation des Zugangs weitere Konten neben dem bereits in SFirm hinterlegten vorhanden sein, erscheint die Frage, ob Sie mit der Auswahl der anzulegenden Konten fortfahren möchten.



Wird dieser Dialog mit <Ja> beantwortet, erscheint erneut der Dialog *HBCI-Konten*, in dem alle noch nicht als Auftraggeberkonto übernommenen Kontoverbindungen zur Auswahl angezeigt werden.



Unmittelbar nach der Bestätigung einer Selektion über die Schaltfläche <OK> erscheint der Dialog *Kontoname ändern*, um den Kontonamen des neuen Kontos ggf. den individuellen Anforderungen anzupassen.

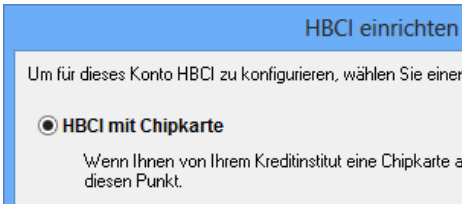


Wird obige Hinweismeldung, dass weitere HBCI-Konten existieren, die noch nicht als Auftraggeberkonten angelegt wurden mit <Nein> beantwortet, erscheint nach Abschluss der Dialoge in der Statuszeile von SFirm ein entsprechender Kundenhinweis. Durch einen Klick auf diesen Eintrag in der Statuszeile wird ein Dialog angezeigt, der Ihnen ggf. Informationen zu aktualisierten HBCI-Benutzerdaten anzeigt (inkl. der Konten, die bisher nicht in SFirm vorhanden waren). In dem Hinweistext haben sie über einen Link die Möglichkeit, direkt zu

der Auftraggeberdatenbank zu wechseln, um die HBCI-Konten als Auftraggeberkonten einzurichten. Möchten Sie die Konten jetzt nicht einrichten, verlassen Sie den Dialog über die Schaltfläche <OK>.

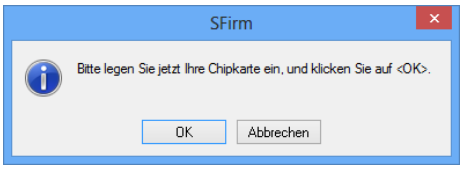
2.2.2 HBCI für ein bestehendes Konto einrichten

Davon ausgehend, dass ein Konto als Auftraggberkonto bereits vorhanden ist und nun *HBCI* als Übertragungsweg in dem Reiter *Übertragung* ausgewählt wird, erscheint ein Assistent, der Sie bei der Einrichtung des Kontos zur Nutzung von HBCI unterstützt.



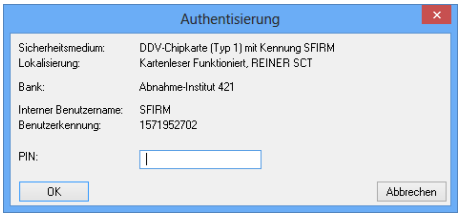
Wählen Sie *HBCI mit Chipkarte* aus und bestätigen Sie <OK>.

Sollte die Chipkarte nicht oder nicht korrekt eingelegt sein, erscheint nebenstehende Hinweismeldung.



Nachdem der Typ der Chipkarte bestimmt wurde, sind für die Einrichtung des HBCI-Zugangs eine Verbindung zu dem Institut und eine Synchronisation des Zugangs erforderlich. Klicken Sie auf <OK> um den Zugang zu synchronisieren.

Die Internetverbindung wird überprüft und die Dialoginitialisierung durchgeführt. Für den Transfer mit dem Institut geben Sie nun die Karten-PIN ein und schließen Sie die Eingabe mit <OK> ab.



Nach einem erfolgreichen Transfer werden die Benutzer- und Verbindungsdaten automatisch in der HBCI-Datenbank hinterlegt.

Alle Informationen zu den Zugangsdaten und Kontoberechtigungen können entweder über *Stammdaten ▸ Bankzugänge ▸ HBCI* oder über das Auftraggeberkonto (*Bankverbindung ändern ▸ HBCI*) eingesehen werden. Nach einem Klick auf <OK> ist die Einrichtung des Kontos für HBCI abgeschlossen.

2.3 HBCI mit einer RAH-Chipkarte konfigurieren

In diesem Abschnitt wird die Einrichtung von HBCI für Chipkarten des Typs RAH-7 (der fast ausschließlich von den Sparkassen/Landesbanken eingesetzt wird) beschrieben. Die Einrichtung entspricht weitestgehend der Beschreibung im Abschnitt HBCI mit einer DDV-Chipkarte konfigurieren. Da sich im Ablauf der Einrichtung jedoch Unterschiede ergeben, wird hier explizit auf RAH-7 eingegangen.

> Bevor die Einrichtung eines RAH-Mediums in SFirm stattfindet, muss die Freischaltung des Zertifikats mit dem HBCI-Service-Client erfolgen. Wenden Sie sich diesbezüglich bitte an Ihren Ansprechpartner bei Ihrer Sparkasse/Landesbank.

2.3.1.1 Unterstützte Chipkartenleser

Folgende Chipkartenleserarten werden unterstützt:

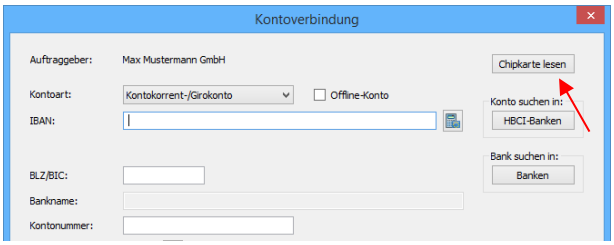
- Secoder-Produkte nach Spezifikation V2.2 im Applikationsmodus
- Klasse-3-Leser mit zwingender PIN-Eingabe über die Lesertastatur, ohne Verwendung des Displays für die Darstellung von Transaktionsdaten
- Klasse-2-Leser mit zwingender PIN-Eingabe über die Lesertastatur

Chipkartenleser ohne Display und Tastatur sowie alte Chipkartenleser mit nicht hinreichenden Sicherheitsfunktionen werden im Rahmen der Zertifikatsaktivierung abgelehnt.

Zur Einrichtung der Kartenleser beachten Sie bitte das Kapitel Kartenleser einstellen.

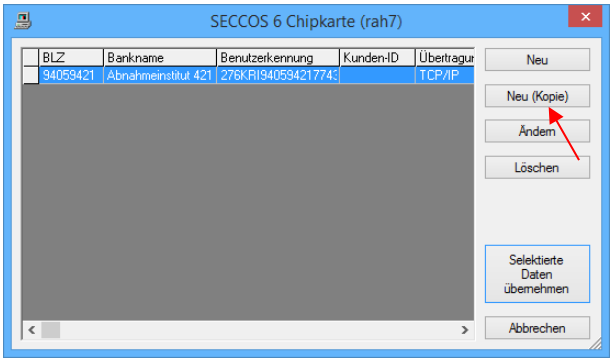
2.3.2 Neuanlage eines Kontos HBCI-Kontos mit einem RAH-7 Medium

Die Einrichtung beginnt über die Schaltfläche <Chipkarte lesen> im Dialog *Kontoverbindung*. Der nebenstehende Dialog erscheint während der Neuanlage eines Auftraggeberkontos.



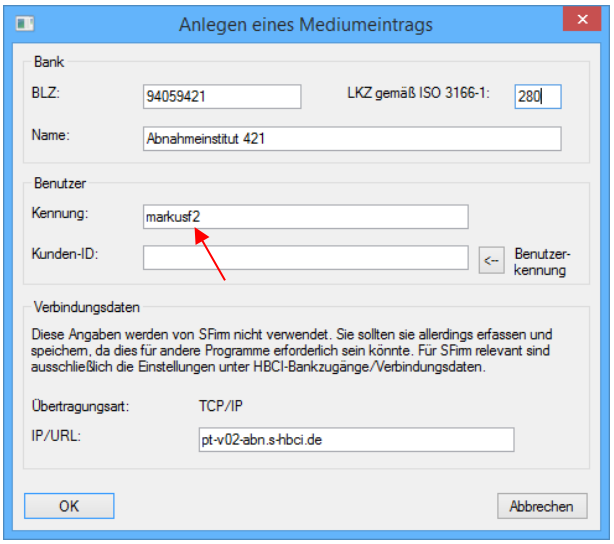
> Dieser Dialog kann nachträglich über die Schaltfläche <Neu> bzw. <Ändern> in dem Reiter *Bankkonten* des Dialogs *Auftraggeber* aufgerufen werden.

Nach der Eingabe der Karten-PIN, werden die auf der Karte befindlichen und für die Anzeige erforderlichen Daten ausgelesen und in dem Dialog *SECCOS 6 Chipkarte (rah7)* angezeigt. Auf der Chipkarte befindet sich i.d.R. bereits ein Datensatz, der durch den HBCI-Service-Client aufgebracht wurde. Erstellen Sie von diesem Datensatz eine Kopie über die Funktion <Neu (Kopie)>.

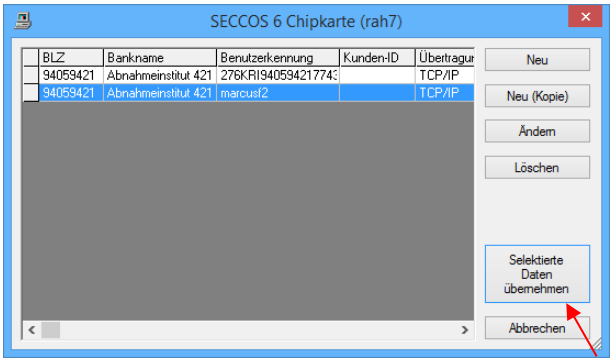


⚠ Der vom HBCI-Service-Client aufgebrachte Datensatz kann nicht übernommen werden. Der Datensatz muss durch <Neu (Kopie)> kopiert werden.

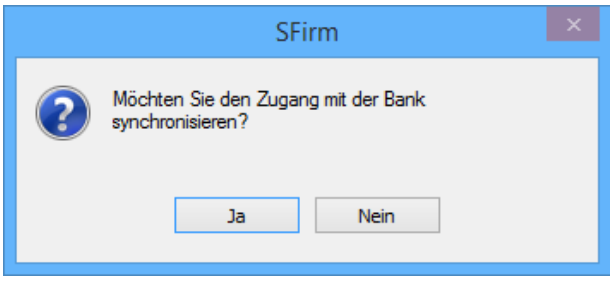
Überschreiben Sie die vorhandene Kennung mit Ihrem persönlichen Anmeldenamen bzw. der Legitimations-ID des HBCI-Vertrags und bestätigen dies bitte mit <OK>.



Nach Selektion des neu angelegten Datensatzes auf der Chipkarte, klicken Sie bitte auf die Schaltfläche <Selektierte Daten übernehmen>.



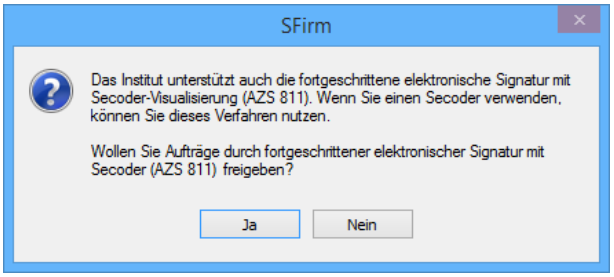
Sie werden anschließend gefragt, ob Sie den Zugang mit der Bank synchronisieren möchten.



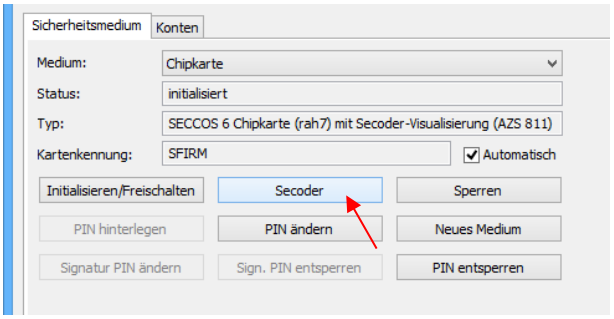
Bestätigen Sie bitte die Meldung mit <Ja>. Nach erfolgter Eingabe der PIN findet der Schlüsselaustausch mit dem Rechenzentrum, sowie das Abholen der Bank- und Benutzerdaten statt.

ℹ Beachten Sie bitte, dass die PIN während des Dialogs mehrfach abgefragt wird. Das resultiert aus dem Verschlüsselungskonzept des Sicherheitsmediums.

Nach dem erfolgreichen Abholen der Bank- und Benutzerdaten kann optional die Verwendung des AZS 811 Verfahrens (Secoder-Visualisierung) aktiviert werden.



Diese können Sie aber auch zu einem späteren Zeitpunkt im HBCI-Benutzer über die Schaltfläche <Secoder> konfigurieren.



Durch die SECODER-Visualisierung werden die Auftragsdaten aus Sicherheitsgründen im Display des Kartenlesers mit SECODER-Funktionalität angezeigt. Zusätzlich ist für die Ausführung eines Auftrags eine mehrfache Bestätigung notwendig.
Für die Nutzung der SECODER-Visualisierung ist es zwingend notwendig, dass der Kartenleser mit dem Typ PC/SC und PIN-Mode 3 eingestellt wurde. Die Nutzung der SECODER-Visualisierung mit einem CT-API-Kartenleser, ist nicht möglich. Zur Konfiguration der Kartenleser beachten Sie bitte das Kapitel Kartenleser einstellen.

Nach einem erfolgreichen Transfer wird die HBCI-Kommunikation beendet und es erscheint eine Auswahl der verfügbaren Konten des Karteninhabers für dieses Institut in dem Dialog *HBCI Konten*. Die Einrichtung entspricht weitestgehend der Beschreibung im Abschnitt HBCI mit einer DDV-Chipkarte konfigurieren.

2.4 Kontoanlage mit einer RDH-Chipkarte

Im Gegensatz zu einer Chipkarte muss der Benutzer eines RDH-Mediums sein Medium im Allgemeinen selbst erstellen.

Der Assistent erkennt, ob das Medium bereits teilinitialisiert ist. Es entfallen dann die entsprechenden Arbeitsschritte.

Im Folgenden wird auf die Varianten näher eingegangen, die den überwiegenden Teil der zum Einsatz kommenden RDH-Karten abdecken sollte:

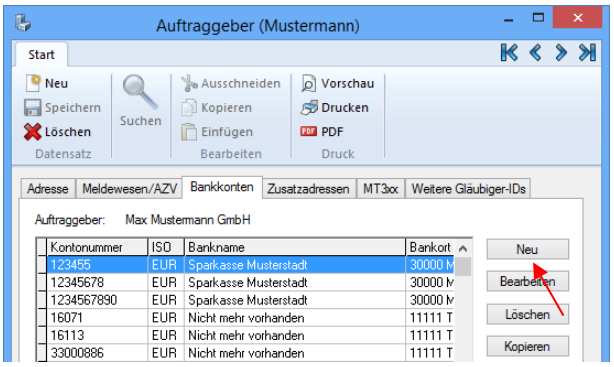
Kontoanlage mit einer vorbelegten RDH-Karte	Diese Variante beschreibt die Kontoanlage mit einer RDH-Karte, die bereits alle notwendigen Daten enthält (also die Bankdaten, Schlüssel und PIN). Weitere Informationen entnehmen Sie bitte dem folgenden Unterkapitel.
Kontoanlage mit einer leeren RDH-Karte	Eine Beschreibung zu der Kontoanlage mit einer leeren RDH-Karte, in der also keine Bankdaten und keine Schlüssel hinterlegt sind und

	die PIN noch nicht gespeichert ist, befindet sich in dem Abschnitt Kontoanlage mit einer leeren RDH-Karte.
Kontoanlage mit einer SECCOS RDH-Karte	Bei der Einrichtung einer SECCOS RDH-Karte ist die sog. Transport-PIN zu berücksichtigen. Weiterhin ist das Vorhandensein oder nicht Vorhandensein von Zertifikaten (Schlüssel) bei der Einrichtung von Bedeutung. Diese Variante wird in dem Abschnitt Einrichtung mit einer SECCOS-Karte behandelt.

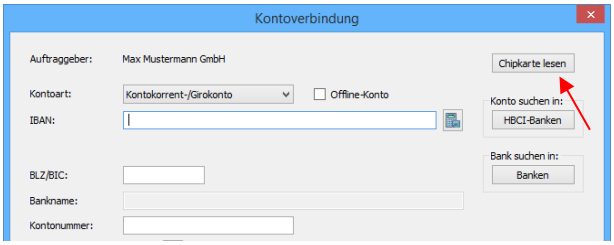
2.4.1 Kontoanlage mit einer vorbelegten RDH-Karte

Die Kontoanlage mit einer vollständig vorbelegten RDH-Karte unterscheidet sich im Wesentlichen nicht von der Anlage mit einer DDV/RAH7-Chipkarte. In diesem Fall sind die Schlüsseldaten bereits vorhanden und die PIN bereits gespeichert. Die Vorgehensweise kann wie folgt aussehen:

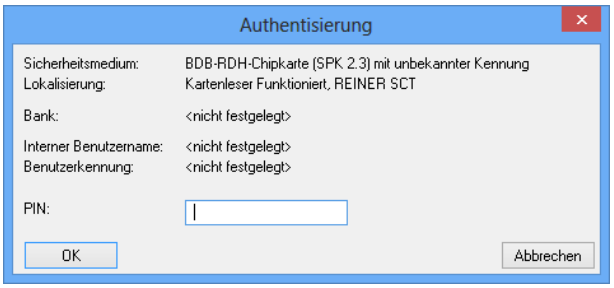
Öffnen Sie über *Stammdaten ▸ Auftraggeber* mit einem Doppelklick den Auftraggeber, dem Sie das Konto zuordnen wollen. Auf dem Reiter *Bankkonten* sehen Sie zunächst nur die bereits eingerichteten Konten. Über die Schaltfläche <Neu> gelangen Sie zu dem Dialog *Kontoverbindung*.



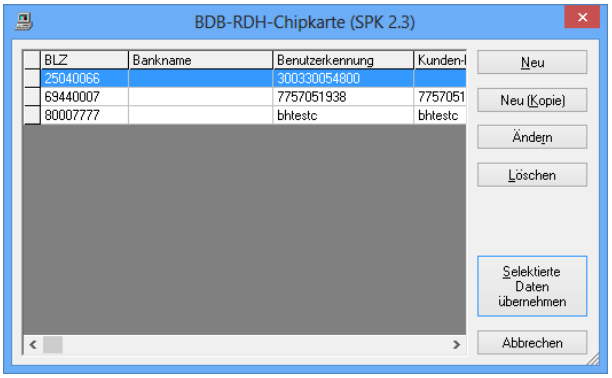
In der leeren Erfassungsmaske zur Neuanlage eines Kontos sehen Sie auf der rechten Seite mehrere Schaltflächen. Klicken Sie hier auf die Schaltfläche <Chipkarte lesen>.



Zur Authentisierung des Kartenzugriffs wird die PIN abgefragt. Nach der Eingabe der PIN und der Bestätigung über die Schaltfläche <OK> werden die Bankdaten, die auf der Karte enthalten sind, angezeigt.

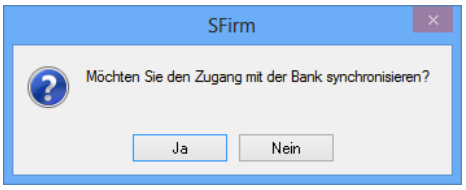


In dem Dialogtitel wird die Bezeichnung des Sicherheitsmediums eingeblendet In der Regel findet sich dort nur ein Eintrag. Wählen Sie bei mehreren den entsprechenden aus (durch ein Kreuz in der ersten Spalte markieren) und klicken Sie auf die Schaltfläche <Selektierte Daten übernehmen>.



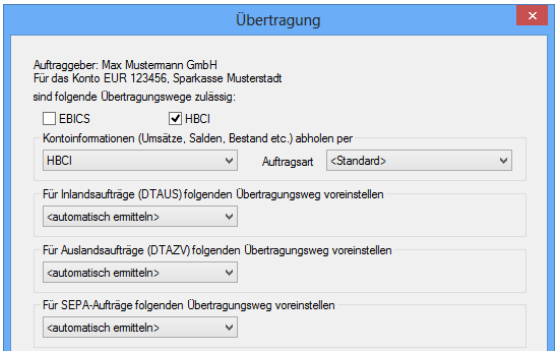
2.4.1.1 Selektierte Daten übernehmen

Anschließend können Sie den Zugang synchronisieren. Bestätigen Sie hierzu den nebenstehenden Dialog mit <Ja>.



Nach einem erfolgreichen Transfer wird die HBCI-Kommunikation beendet und es erscheint eine Auswahl der verfügbaren Konten des Karteninhabers für dieses Institut in dem Dialog *HBCI Konten*.

Nach der Selektion eines Kontos und der Bestätigung der Schaltfläche <OK>, erscheint der Dialog *Übertragung*. Der Übertragungsweg *HBCI* wird nun automatisch markiert angezeigt. Ebenso auch die Abholung der Kontoumsätze per HBCI. Automatisch ermittelt wird der Übertragungsweg für den Transfer von DTAUS und DTAZV und SEPA-Aufträgen.



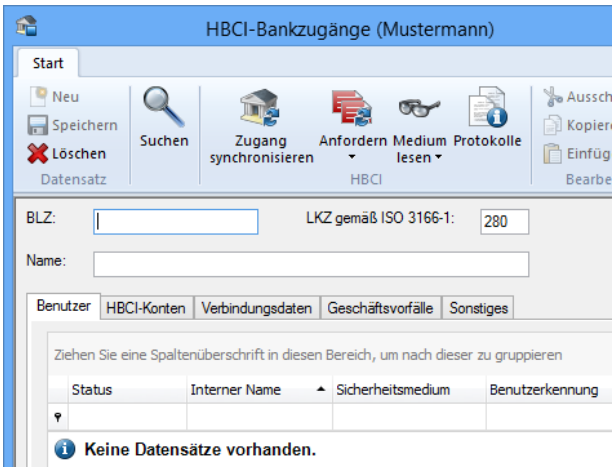
Mit den <Weiter>-Schaltflächen werden weitere Dialoge angezeigt. Zu diesen gehören je nach lizenzierten Modulen die Dialoge *Cash*, *Depooling*, *AZV*, *MT101*, *HBCI*, und *Rundrufdefinition*. Nach Bestätigung der Schaltfläche <Fertig stellen> ist die Kontoanlage abgeschlossen. Sollten mit der Synchronisation des Zugangs weitere Konten neben dem bereits in SFirm hinterlegten vorhanden sein, erscheint eine Meldung, die Sie auf diesen Umstand aufmerksam macht und die Anlage dieser weiteren Konten anbietet. Die weiteren Schritte, die je nach Beantwortung dieser Hinweismeldung folgen, werden in dem Abschnitt Weitere Konten des gleichen Instituts einbinden beschrieben.

2.4.2 Kontoanlage mit einer leeren RDH-Karte

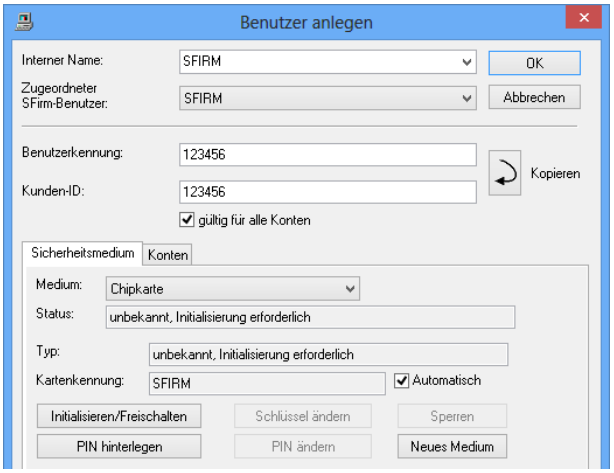
In diesem Abschnitt wird eine Kontoanlage mit einer leeren RDH-Karte beschrieben, die keine Bankdaten, keine Benutzerkennung und keine Schlüssel enthält. Die Karten-PIN wurde ebenfalls noch nicht hinterlegt. Zur besseren Übersicht wird die Einrichtung hier über *Stammdaten ▸ Bankzugänge ▸ HBCI ▸ HBCI-Bankzugang ▸ Neu* vorgenommen.

2.4.2.1 HBCI-Bankzugang und HBCI-Benutzer anlegen

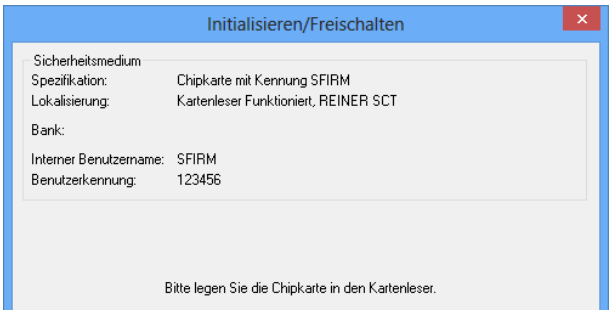
Geben Sie zunächst in dem Dialog *HBCI-Bankzugang* die BLZ der betreffenden Bank ein. Ist das Institut bekannt, wird das Feld *Name:* mit Betätigung der TAB- oder Enter-Taste von SFirm automatisch gefüllt.



Über die Schaltfläche <Neu> im Reiter *Benutzer* öffnen Sie nun den Dialog *Benutzer anlegen*. Die Benutzerkennung und Verbindungsdaten werden Ihnen vom Kundenberater mitgeteilt und hier erfasst. Die Angaben der Benutzerkennung sind nur für die Initialisierung erforderlich. Legen Sie nun die Chipkarte ein und klicken Sie auf die Schaltfläche <Initialisieren/Freischalten>.

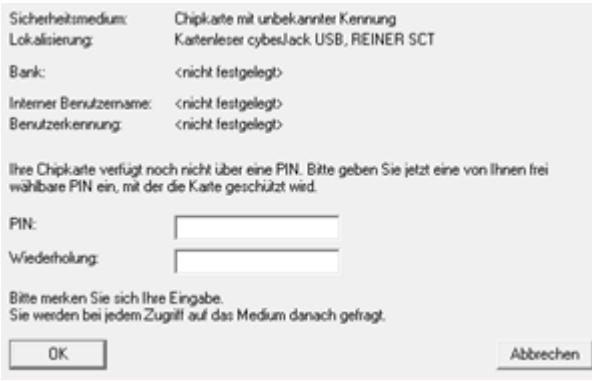


Nachdem die Verbindungsdaten manuell angelegt oder erfolgreich abgeholt wurden, erscheint nebenstehender Dialog, in dem die Daten des Sicherheitsmediums angezeigt werden. Legen Sie nun die Chipkarte ein und klicken Sie auf <Weiter>.



2.4.2.2 Die PIN hinterlegen

Nachdem der Typ der Karte bestimmt wurde, ist in dem Dialog *Authentisierung* die (fünf- bis achtstellige nummerische) Karten-PIN einzugeben und durch eine Wiederholung zu bestätigen. Klicken Sie anschließend auf <OK>. Die PIN wird später für die Autorisierung von Aufträgen verwendet.



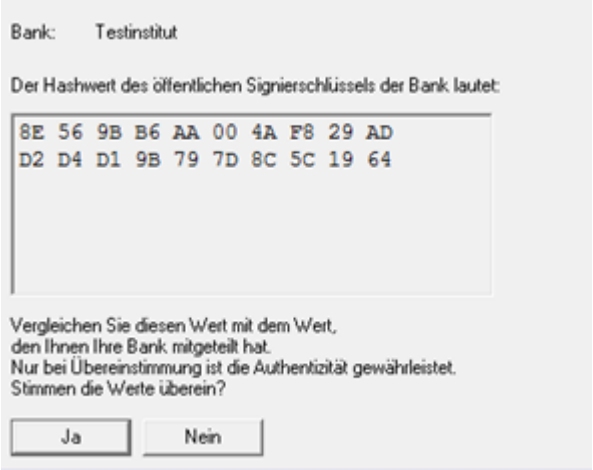
2.4.2.3 Initialisieren und Freischalten

Die Karten-PIN wird nun auf die Karte geschrieben. Neben der Anzeige des Kartentyps wird nun darauf hingewiesen, dass noch keine Daten (Schlüssel) auf der Karte vorhanden sind. Klicken Sie auf <Weiter>.

Es folgt eine Meldung, dass die Benutzerdaten und Benutzerschlüssel (ein persönlicher Schlüssel und ein öffentlicher Schlüssel) auf dem Sicherheitsmedium erfolgreich angelegt wurden. Dieser Vorgang kann bis zu einigen Minuten dauern. Klicken Sie nun auf <Weiter>.

Sie werden vor dem Austausch der Schlüssel mit der Bank erneut dazu aufgefordert, das Sicherheitsmedium einzulegen. Klicken Sie anschließend auf <Weiter>.

Sobald der öffentliche Bankschlüssel empfangen wurde, erhalten Sie in dem Dialog *Bankschlüssel bestätigen* die Hash-Werte als Prüfsumme, um den Schlüssel eindeutig zu identifizieren. Diese Angaben vergleichen Sie bitte mit den Angaben im INI-Brief des Instituts und bestätigen bei Korrektheit die Schaltfläche <Ja>. Sollten Die Werte nicht übereinstimmen, so sollte dies mit dem Institut abgeklärt werden.



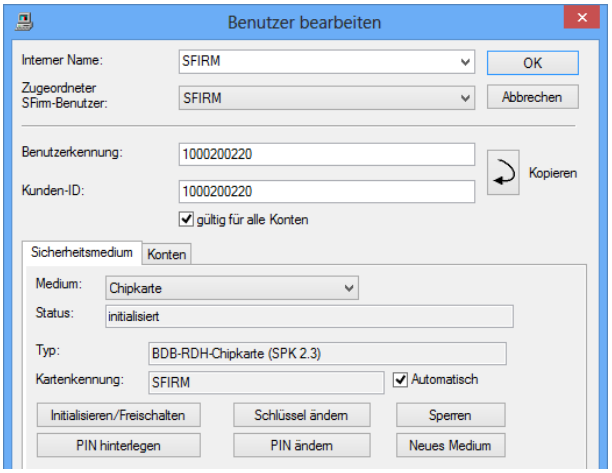
Die zur Bank übertragenen Benutzerschlüssel werden in den vom Programm erstellten INI-Brief übernommen, der die Legitimation für die Initialisierung des Kontos und für die Freischaltung Ihrer Schlüssel darstellt. Drucken Sie den Brief über die Schaltfläche <INI-Brief drucken> aus. Dieser Brief ist unterschrieben an das Institut weiterzuleiten.

Die Freischaltung der Benutzerschlüssel kann auf Institutsseite mehrere Tage in Anspruch nehmen.

SFirm erkennt anhand der ausgetauschten Daten, ob der Ausdruck eines INI-Briefes erforderlich ist oder nicht. Dies kann z.B. bei Verwendung RDH-3 / VR-NetWorld-Cards nach dem Schlüsselaustausch und nach Erhalt eines Zertifikats der Fall sein. Das RZ kann dann sofort die Authentizität des Schlüssels feststellen. Der im obigen Dialog angezeigte Text (oberhalb der Schaltfläche <INI-Brief drucken>) ändert sich dann wie folgt:

Sie können den Benutzerschlüssel bei Ihrer Bank bestätigen. Dies kann durch einen INI-Brief geschehen, den Sie hier drucken können. Nach SFirm vorliegenden Informationen ist das aber nicht oder nicht mehr erforderlich.

Nach Abschluss dieser Prozedur befinden Sie sich wieder in dem Dialog Benutzer bearbeiten. Schließen Sie den Dialog nun über <OK>. Nach der Freischaltung muss nun der Zugang synchronisiert werden, um später die Zahlungsaufträge signieren bzw. die Kontoumsätze abrufen zu können.



2.4.2.4 Weitere Konten hinterlegen und Abschluss der Einrichtung

Um alle Konten nach der Synchronisation des Zugangs beim Auftraggeber zu hinterlegen, sind die Schritte durchzuführen, die bereits weiter oben beschrieben wurden.

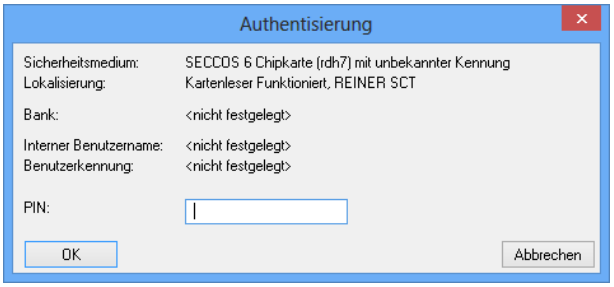
Mit den <Weiter>-Schaltflächen werden weitere Dialoge angezeigt. Zu diesen gehören je nach lizenzierten Modulen die Dialoge *Cash*, *Depooling*, *AZV*, *MT101*, *HBCI*, und *Rundrufdefinition*. Nach Bestätigung der Schaltfläche <Fertig stellen> ist die Kontoanlage abgeschlossen. Sollten mit der Synchronisation des Zugangs weitere Konten neben dem bereits in SFirm hinterlegten vorhanden sein, können Sie mit der Anlage dieser Konten jetzt fortfahren. Die weiteren Schritte, die je nach Beantwortung dieser Hinweismeldung folgen, werden in dem Abschnitt Weitere Konten des gleichen Instituts einbinden beschrieben.

2.4.3 Einrichtung mit einer SECCOS-Karte

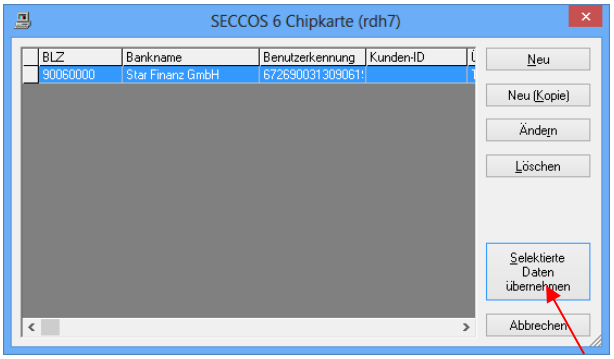
2.4.3.1 SECCOS-Karte (RH-7)

Sie erhalten die Karte und eine dazu gehörige 6-stellige PIN. Sie haben die Möglichkeit diese PIN zu ändern, dies ist jedoch nicht erforderlich.

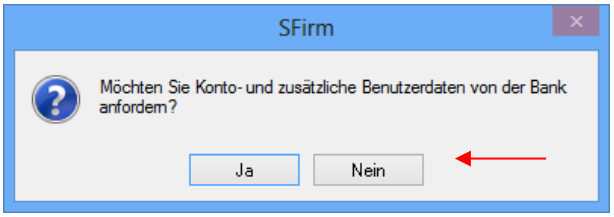
Beim Lesen der Karte innerhalb des HBCI-Bankzugangs geben Sie bitte die 6-stellige Karten-PIN ein.



Im nächsten Schritt erscheint die Auflistung der auf der HBCI-Karte vorhandenen Datensätze. Markieren Sie den gewünschten Datensatz und klicken bitte auf <Selektierte Daten übernehmen>

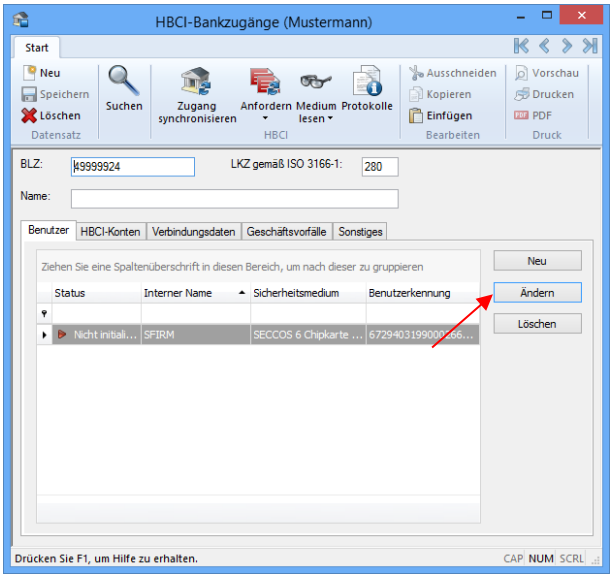


Die Frage im nebenstehenden Dialog beantworten Sie bitte mit <Nein>



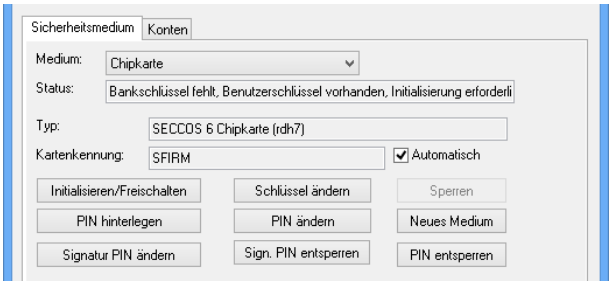
Der Datensatz ist jetzt in dem HBCI-Bankzugang angelegt, es fehlt jedoch noch die Initialisierung.

Klicken Sie bitte auf <Ändern> um in den Dialog <Benutzer bearbeiten> zu gelangen.



Um das Medium zu initialisieren, klicken Sie bitte auf <Initialisieren/Freischalten>.

Im Laufe des Dialogs werden Sie aufgefordert die PIN einzugeben.



War der Vorgang erfolgreich, erscheint der Hashwert.

Der INI-Brief muss an dieser Stelle nicht gedruckt werden, da Ihnen dieser i.d.R. bereits im Voraus zugesendet wurde.

Klicken Sie auf <Beenden>. Der Status des Benutzers sollte jetzt auf *initialisiert* stehen.

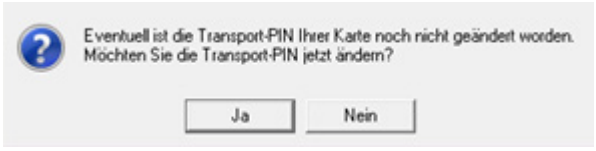
Nach der Synchronisation des Zugangs ist das Medium einsatzbereit.

2.4.3.2 SECCOS-Karte (RDH-9)

Sie erhalten in einem separaten Bankbrief eine (5-Stellige) sog. Transport-PIN mitgeteilt. Eine Karten-PIN wird nicht mitgeliefert, da diese vom Benutzer selbst vergeben werden muss.

Beim ersten Kartenzugriff wird i.d.R. vom Anwender die Transport-PIN eingegeben. Entscheidend ist, dass SFirm nun feststellt, dass noch keine gültige Karten-PIN auf der Karte hinterlegt ist und daher nebenstehenden Dialog anzeigt.

Um die SECCOS-Karte für SFirm verwenden zu können muss die Transport-PIN in eine individuelle Karten-PIN geändert werden. Klicken Sie also auf <Ja>.



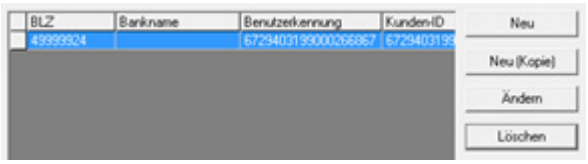
Es erscheint ein Hinweisdialog mit Informationen zur Änderung der Transport-PIN um eine Falscheingabe und damit u.U. einer Kartensperrung zuvor zu kommen. Bestätigen Sie die Meldung mit <OK>.

Als erstes ist jetzt (wie in der Hinweismeldung angegeben) die 5-Stellige Transport-PIN einzugeben. Bestätigen Sie die Eingabe anschließend mit der Schaltfläche <OK>.

Im folgenden Dialog ist nun eine vom Benutzer selbst kreierte numerische Karten-PIN einzugeben, die in Zukunft für den Kartenzugriff Verwendung finden soll. Die PIN-Länge muss aus 6 bis 8 Zahlen bestehen. Aufgrund der verdeckten Eingabe, muss diese wiederholt werden. Bestätigen Sie anschließend die Eingaben mit der Schaltfläche <OK>.

Es erscheint nun eine Erfolgsmeldung, die zusätzlich darauf hinweist, dass ab sofort nur noch die vom Benutzer selbst gewählte Karten-PIN Verwendung finden muss.

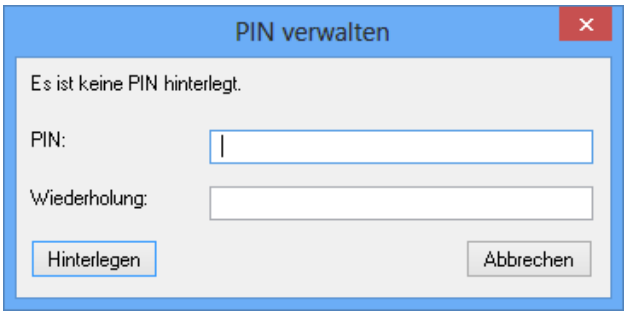
Nach der Bestätigung dieser Meldung, gelangen Sie in die Übersicht (hier *SECCOS Chipkarte (rdh9)*).



Der weitere Ablauf der Einrichtung entspricht weitestgehend der Beschreibung im Abschnitt Selektierte Daten übernehmen.

2.5 Pin/Passwort verwalten (HBCI)

In dem HBCI-Bankzugang innerhalb des Dialogs *Benutzer Bearbeiten* haben Sie die Möglichkeit das Passwort (bei Sicherheitsdateien) oder die PIN (bei Chipkarten) zu hinterlegen. Geben Sie die PIN im Feld *PIN* ein und wiederholen diese PIN zur Kontrolle im Feld *Wiederholung*. Dann betätigen sie die Schaltfläche <Hinterlegen>.



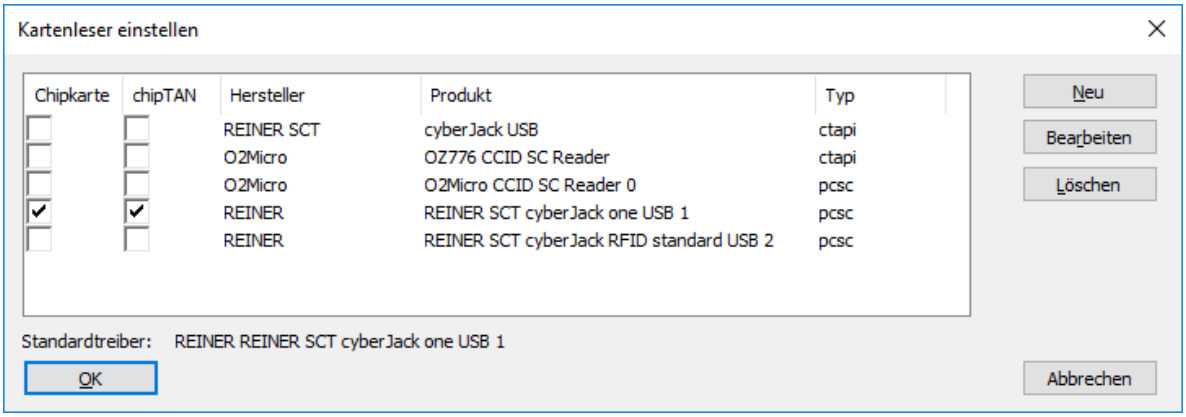
Sofern Sie keinen Klasse-2-Kartenleser verwenden und ein PIN hinterlegt haben, entfallen bei Zugriffen auf die Chipkarte die Aufforderungen zur PIN-Eingabe. Bitte beachten Sie, dass durch das Hinterlegen einer PIN das Risiko einer unbefugten Benutzung des Sicherheitsmediums besteht.

2.6 Kartenleser einstellen

Neben dem Zugang über den Verbindungsassistenten ist ein separater bzw. nachträglicher Aufruf auch über das Menüband *Wartungscenter ▸ Konfiguration ▸ Kartenleser* möglich.

Die Installation des Kartenlesers erfolgt grundsätzlich außerhalb von SFirm. Es muss eine Treibersoftware für den Leser geladen werden. SFirm wird nur die Schnittstelle für den Leser mitgeteilt, und welcher Leser – bei mehreren installierten Treibern – der aktive Treiber ist.

Im Menüband *Wartungscenter ▸ Konfiguration* wird in der Funktion *Kartenleser* der Chipkartenleser für die Verfahren HBCI bzw. EBICS zugeordnet. Wenn die Autorisierung über Chipkarten erfolgt, müssen Sie für den Kartenleser die vom Hersteller gelieferten Treiber bereits vor der Konfiguration von SFirm installieren. Grundsätzlich wird jeder Kartenleser unterstützt, dessen Treiber das PC/SC und /oder CT-API-Interface zur Verfügung stellt.

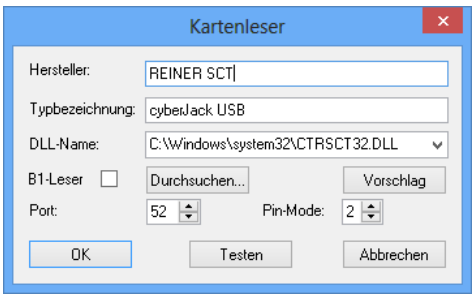


Sie sehen die in SFirm eingerichteten Kartenleser. Einige Kartenleser unterstützen sowohl das HBCI-Chipkartenverfahren (DDV, RAH, RDH), wie auch die chipTAN USB Funktionalität. Es gibt aber auch Kartenleser, die nur eines der beiden Verfahren unterstützen. In diesen Fällen muss festgelegt werden, welcher Kartenleser die unterschiedlichen Verfahren bedienen.

Beachten Sie bitte, dass es nicht möglich ist, mehrere Karteleser für ein Verfahren zu wählen. Es kann immer nur ein Kartenleser pro Verfahren (Chipkarte/chipTAN) aktiv sein.

2.6.1.1 CT-API

Treiber, die nicht in der Liste enthalten sind müssen mit der Schaltfläche <Neu> angelegt werden. Es erscheint ein Dialog, in dem die geforderten Treiberdaten eingegeben werden. Die Felder des Dialogs *Kartenleser* im Einzelnen:



Hersteller	Geben Sie hier einen individuellen Text für den Hersteller ein. Der Inhalt dieses Feldes hat einen rein informativen Charakter und kann beliebig gefüllt werden.
Typ	Geben Sie hier einen individuellen Text für den Typ des Kartenlesers ein. Der Inhalt dieses Feldes hat einen rein informativen Charakter und kann beliebig gefüllt werden.
DLL-Name	Im Feld *DLL-Name* ist der vollständige Pfad der Treiber-DLL anzugeben, der für den Kartenleser zuständig ist. Diese DLL muss das CT-API-Interface zur Verfügung stellen. Diese DLL befindet sich üblicherweise im Windows-Verzeichnis, im System-Verzeichnis oder im Installations-Verzeichnis der Treibersoftware. Informieren Sie sich im Zweifel beim Hersteller des Lesers. Zur Bestimmung der DLL werden Sie von den Schaltflächen <Durchsuchen> und <Vorschlag> unterstützt.
B1-Leser	Diese Einstellung ist zu markieren, wenn ein B1-Leser vorliegt. Informieren Sie sich im Zweifel beim Hersteller des Lesers.
<Durchsuchen…>	Es erscheint ein Standard-Dateidialog zur Suche nach DLLs. Sie auch folgenden Abschnitt *Programmbibliotheken*.
<Vorschlag>	Mit <Vorschlag> erhalten Sie eine Auflistung der DLLs im Windows- und Systemverzeichnis, die diese CT-API zur Verfügung stellen. Es werden diese Verzeichnisse ausgelesen, weil die Hersteller die Dateien meist in diese Ordner kopieren. Falls mehrere Dateien gefunden werden, können Sie i.d.R. am Namen der Dateien erkennen, ob es sich um die benötigte 32Bit-DLL handelt. Bei Bedarf sollten Sie den Treiber durch die Konfiguration von Parametern und das Lesen der Karte prüfen.
Port [ ]	Der Wert des Ports ist i.d.R. ein interner Wert des Treibers und wird im Allgemeinen auch vom Treiber vorgegeben. Wenn Probleme mit dem Kartenleser auftreten, kann der Wert variiert werden.
PIN-Mode [ ]	Der PIN-Modus bietet mit dem Wert *0* keine weiteren Sicherheitsmechanismen des Lesers. Mit dem Wert *1* besitzt der Leser eine Kopplung zwischen Tastatur und PC. Mit Wert *2* hat der Leser eine eigene Tastatur und ggf. auch ein Display. Beim Wert *3* verfügt der Leser über Tastatur und Display und evtl. über ein personalisiertes Sicherheitsmodul mit RSA-Funktion, das eine weitere Signatur benötigt. Die Einbettung dieser Kartenlesersignatur in die Anwendung erfolgt durch anwendungsspezifische Zusatzfunktionen im Leser.
<Testen>	Mit der Schaltfläche <Testen> kann die korrekte Einstellung geprüft werden. Dazu ist es erforderlich, eine beliebige Chipkarte in den Kartenleser einzulegen. Es wird lediglich ein sog. INIT auf die Karte durchgeführt.

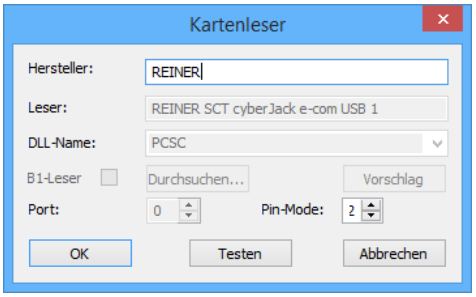
Programmbibliotheken

Über die Schaltfläche <Vorschlag…> erreichen Sie den Dialog *Programmbibliotheken*. Wie beschrieben werden alle Programmbibliotheken mit einem CT-API Interface aus dem Windows bzw. Systemverzeichnis aufgelistet. In den meisten Fällen wird der Installation Ihres Kartenlesers eine Treiber-DLL mit einer Implementierung des CT-API-Interfaces in das Windows- oder das Systemverzeichnis kopiert.

Diese Treiber-DLL ist von Ihnen auszuwählen. Im Zweifel wenden Sie sich bitte an den Hersteller Ihres Kartenlesers.

2.6.1.2 PC/SC

Bei Kartenlesern, die über die PC/SC-Schnittstelle angesprochen werden, besteht aus Sicherheitsgründen nur eine eingeschränkte Möglichkeit der Konfiguration. Bei dieser Schnittstelle ist eine Manuelle Konfiguration nicht nötig.



Dieser Modus ist für die Nutzung der SECODER-Visualisierung obligatorisch.

2.6.2 Kartenleser in Remotedesktopserver-Umgebungen

2.6.2.1 Allgemeines

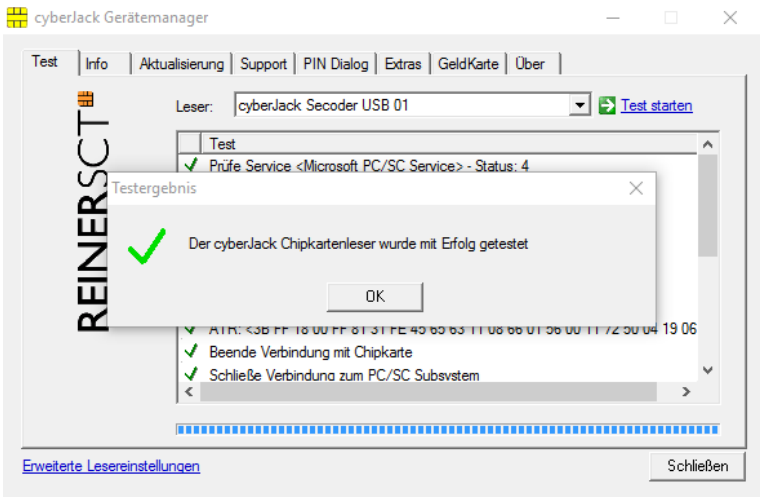
Grundsätzlich ist die Verwendung von Kartenlesern in einer Remotedesktopsitzung möglich, somit auch der Übertragungsweg HBCI per Chipkarte/Sicherheitsdatei oder EBICS mit elektronischer Unterschrift auf Chipkarte.

⚠ Die Einrichtung und Konfiguration üblicher Kartenlesegeräten sollte durch einen fachkundigen Systemadministrator durchgeführt werden. Da sich die Einrichtung, in unserer Testumgebung, teilweise als sehr schwierig gestaltet hat und dessen Erfolg von vielen Systemumgebungsfaktoren abhängt, können wir hierzu lediglich bedingt Support leisten.

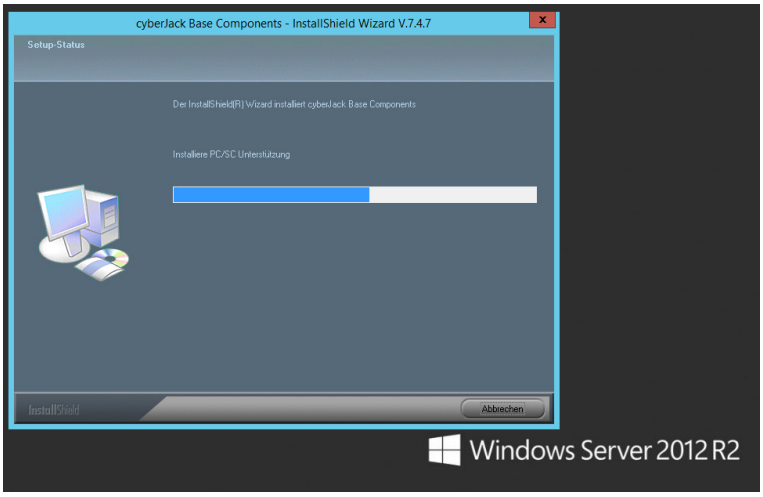
2.6.2.2 Einrichtung

In dem folgenden Abschnitt wird das Hinzufügen eines Remotekartenleser in eine Remotedesktopsitzung am Beispiel von Kartenlesern der Firma Reiner SCT.

Zunächst muss der Kartenleser am Client angeschlossen werden. Anschließend müssen die erforderlichen Gerätetreiber vom Hersteller heruntergeladen und installiert werden. Es sollte über die entsprechende Verwaltungssoftware (z.B. cyberJack Gerätemanager) sichergestellt werden, dass der Kartenleser erkannt wird und auch über die aktuelle Firmware verfügt.



Auf dem Remotedesktop-, bzw. Citrix-Server, auf dem SFirm installiert ist und der Kartenleser verwendet werden soll, muss ebenfalls der Kartenlesertreiber des Herstellers installiert werden. Damit stehen den installierten Programmen auf dem Remotedesktopserver alle Funktionalitäten des Kartenlesertreibers zur Verfügung.

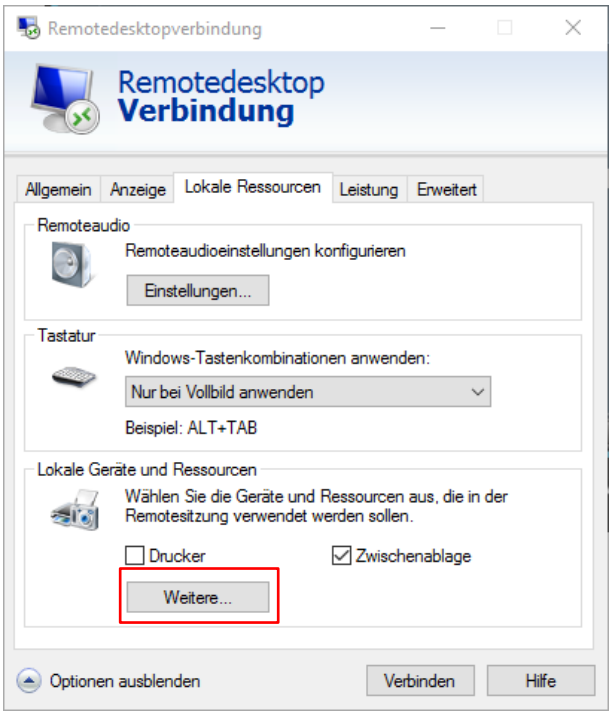


Genaue Spezifikationen und eventuelle Einschränkungen der Funktionalitäten sind den Internetseiten des Kartenleser-Herstellers oder über deren Kundenservice zu erfragen.

Damit der Kartenleser über eine Remotedesktopsitzung verfügbar ist, muss dieser als lokale Ressource in der Remotedesktopsitzung verfügbar gemacht werden.

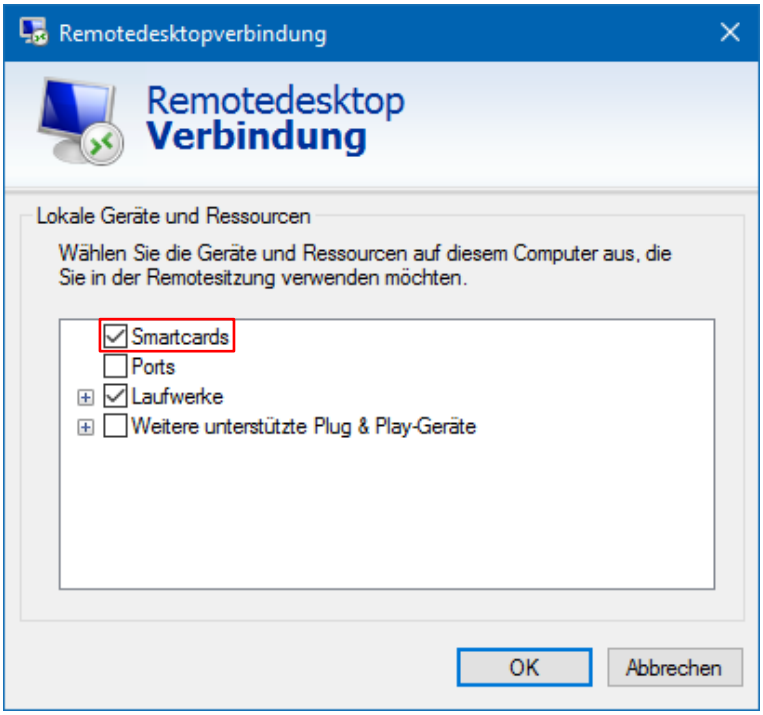
Dies ist in der Einrichtung vergleichbar mit lokalen Laufwerken. Im Regelfall ist diese Einstellung bereits aktiv.

Diese Einstellung kann der Anwender in der Remotedesktopverbindung durchführen oder die Systemadministratoren haben die Möglichkeit, dieses für den Anwender vorzugeben. Diese Möglichkeit bestehen sowohl für Remotedesktopverbindungen, als auch Anwendungen die per Citrix-XenApp/XenDesktop veröffentlicht werden.



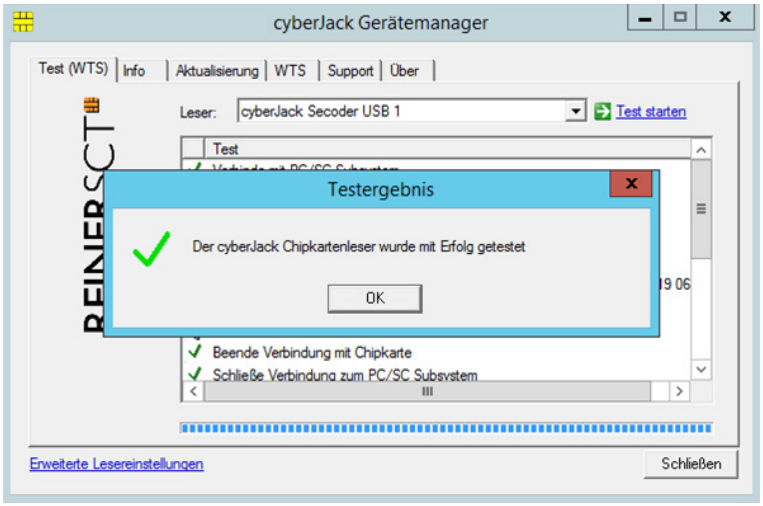
Im Regelfall ist diese Einstellung bereits aktiv. Diese Einstellung kann der Anwender in der Remotedesktopverbindung durchführen oder die Systemadministratoren haben die Möglichkeit, dieses für den Anwender vorzugeben.

Diese Möglichkeit bestehen sowohl für Remotedesktopverbindungen, als auch Anwendungen die per Citrix-XenApp/XenDesktop veröffentlicht werden.

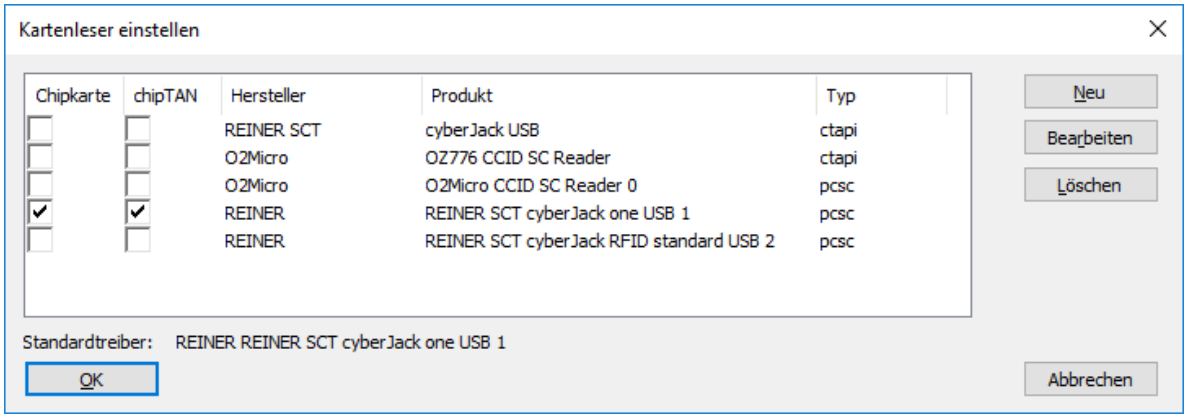


In SFirm ist direkt nach der Installation des Kartenlesertreibers ein neuer Kartenleser des Typs CT-API verfügbar. Erst wenn die o.g. Smartcard-Einstellung aktiv ist, wird ein weiterer Kartenleser des Typs PC/SC sichtbar.

Wenn die Einstellungen entsprechend gesetzt sind, kann nach der Anmeldung über die Remotedesktopverbindung oder Citrix ein Funktionstest über den Gerätemanager durchgeführt werden. Hierzu sollte eine entsprechende Karte im Kartenleser stecken oder verfügbar sein.



Wir empfehlen grundsätzlich die Nutzung und Aktivierung des Kartenleser-Typs PC/SC innerhalb von SFirm:



Führen Sie abschließend bitte einen Kartenlesertest in SFirm durch. Verlief dieser positiv, ist die Einrichtung abgeschlossen.

3 HBCI mit Sicherheitsdatei einrichten

Mit HBCI-Sicherheitsdatei werden alle Daten komplett verschlüsselt sowie zur Sicherung der Authentizität signiert. Sollen die Schlüssel als Sicherheitsdatei auf einem Datenträger (z.B. einem USB-Stick oder auf der Festplatte) gespeichert werden, wird die Konfiguration wie folgt vorgenommen.

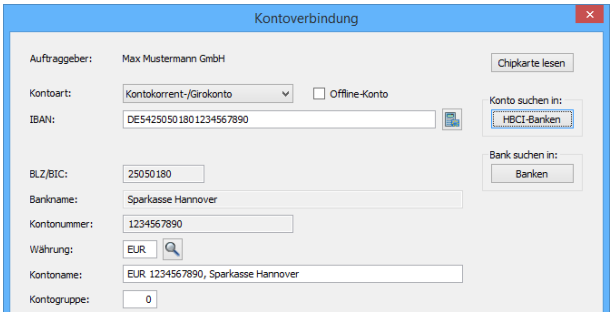
3.1 Voraussetzungen

Konfiguration der Übertragungswege	Die Konfiguration des Übertragungsweges für HBCI mit Sicherheitsdatei wird hier vorausgesetzt.

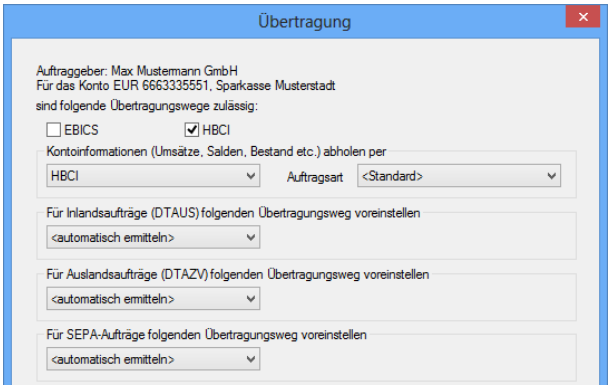
3.2 Erfassung einer Kontoverbindung

Beachten Sie bitte, dass die Benutzerschlüssel von dem in SFirm angemeldeten Benutzer selbst generiert werden müssen. Eine entsprechende Anmeldung sollte also vorliegen.

Erfassen Sie zunächst über *Stammdaten ▸ Auftraggeber* (Reiter *Bankkonten)* im Dialog *Kontoverbindung* die Kontodaten.

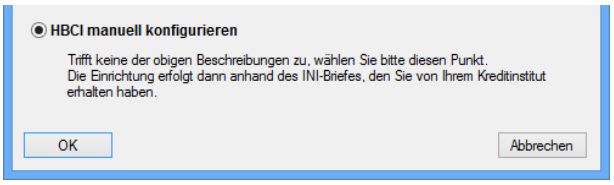


Als Übertragungsweg ist das Verfahren *HBCI* auszuwählen. Das Abholen der Kontoumsätze mit HBCI wird automatisch vorbelegt. Klicken Sie auf <Weiter> und definieren Sie die Parameter für die weiteren Module von SFirm.



3.3 Der Assistent zur manuellen Konfiguration

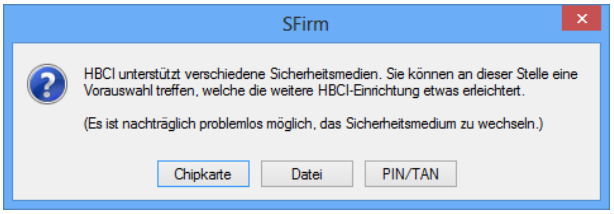
Ein Assistent unterstützt Sie bei der Konfiguration. Wählen Sie in dem Dialog *HBCI einrichten* die unterste Funktion *HBCI manuell konfigurieren* aus und bestätigen Sie die Auswahl mit der Schaltfläche <OK>.



I.d.R. werden die Angaben des vorbelegten Instituts übernommen und können mit <OK> bestätigt werden.

Anschließend werden die Benutzer- und Verbindungsdaten definiert, die Ihnen vom Institut bzw. dem Kundenberater mitgeteilt werden. Bestätigen Sie den Hinweis, ob Benutzerdaten angelegt werden sollen mit <Ja>.

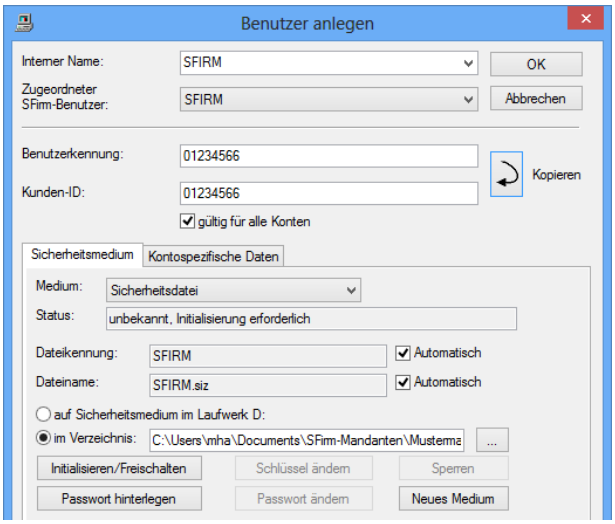
Bestätigen Sie im nächsten Dialog als Sicherheitsmedium <Datei>, damit die Schlüssel auf einer Sicherheitsdatei gespeichert werden.



Es erscheint nun noch ein Hinweis, dass im folgenden Dialog *Benutzer anlegen* die Felder anhand der Angaben des INI-Briefs des Kreditinstituts auszufüllen sind und anschließend die Schaltfläche <OK> zu betätigen ist.

3.4 Einen Benutzer anlegen

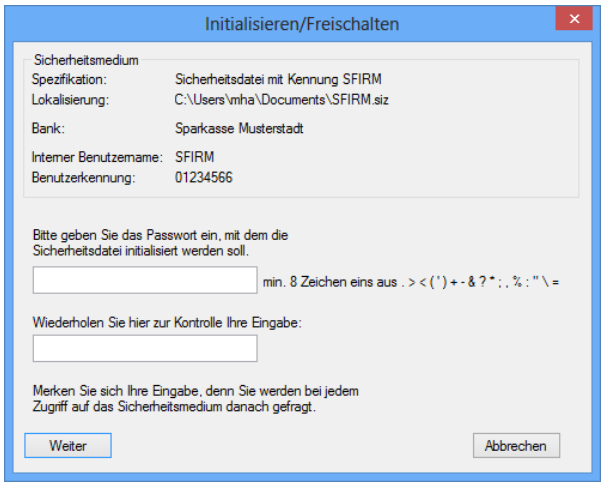
Geben Sie die vom Institut mitgeteilte Benutzerkennung ein. Häufig stimmt die Kunden-ID mit der Benutzerkennung überein. Vergibt die Bank keine Kunden-ID, ist in diesem Fall das Feld mit der Benutzerkennung zu erfassen. Als Medium ist bereits *Sicherheitsdatei* ausgewählt. Das Kontrollfeld *gültig für alle Konten* ist zu aktivieren, wenn die *Kunden-ID* für alle Konten gültig sein soll. Ist das Kontrollfeld deaktiviert, so ist bei jedem verfügbaren Konto eine separate Kunden-ID zu hinterlegen.



Nachdem die Erfassung mit <OK> bestätigt wurde, erscheint ein Hinweis, der Sie zur Initialisierung des Sicherheitsmediums auffordert. Sollten die Übertragungswege in diesem Moment nicht zur Verfügung stehen, können Sie mit <Nein> die Initialisierung zunächst zurückstellen.

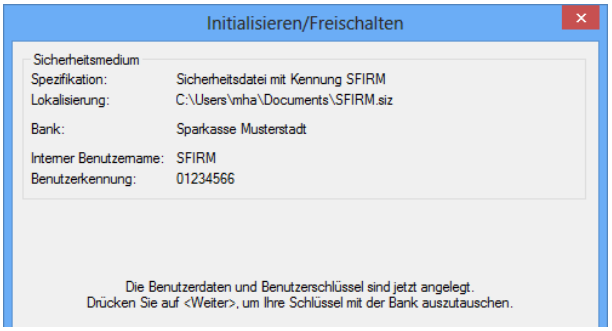
3.5 Initialisieren und Freischalten

Anschließend wird das Passwort definiert, mit dem die Sicherheitsdatei initialisiert wird. Bei der Eingabe müssen aus Sicherheitsgründen mindestens 8 Zeichen und eines der folgenden Sonderzeichen . < > 8) + & ? ; , % : \ = oder “ verwendet werden. Mit <Weiter> werden die Benutzerdaten und -schlüssel auf einen Wechseldatenträger bzw. Festplatte geschrieben und der erfolgreiche Vorgang in einem Hinweisdialog angezeigt. Mit <Weiter> wird eine Verbindung zum Institut aufgebaut.



Der Ablageort der Sicherheitsdatei wurde in dem Dialog *Benutzer anlegen* zuvor Festgelegt.

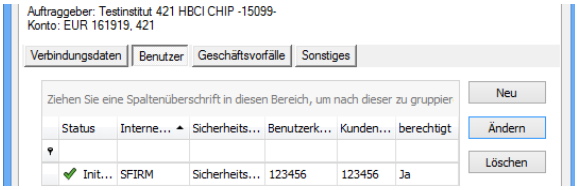
Es wird nun der öffentliche Schlüssel von SFirm an das Institut übertragen und auch der öffentliche Schlüssel vom Institut abgeholt. Für den Transfer benötigen Sie das Schreiben des Instituts zur Prüfung der öffentlichen Schlüsseldaten.



Die zur Bank übertragenen Benutzerschlüssel werden in den vom Programm erstellten INI-Brief übernommen, der die Legitimation für die Initialisierung des Kontos und für die Freischaltung Ihrer Schlüssel darstellt. Drucken Sie den Brief über die Schaltfläche <INI-Brief drucken> aus und leiten Sie diesen mit Ihrer Unterschrift an das Institut weiter.

Beachten Sie, dass nach der Freischaltung noch der Zugang synchronisiert werden muss, um später die Zahlungsaufträge signieren bzw. die Kontoumsätze abrufen zu können.

Um nachträglich die Benutzerdaten abzurufen, wählen Sie im entsprechenden Auftraggeber im Reiter *Bankkonten* die Kontoverbindung aus. Bestätigen Sie <Ändern>. Wählen Sie im Reiter *HBCI* durch einen Mausklick den Benutzer aus und bestätigen Sie die Schaltfläche <Zugang synchronisieren>.



Sie werden aufgefordert, das Sicherheitsmedium auszuwählen / einzulegen und die PIN einzugeben. Mit <OK> erfolgt die Verbindung beim Institut und der Zugang wird synchronisiert. Die Kontoanlage mit einer HBCI-Sicherheitsdatei ist damit abgeschlossen.

Müssen nachträglich neue Benutzer oder fehlende Parameter für einzelne Konten definiert werden, kann dies entweder bei der Kontoverbindung des Auftraggebers oder über *Stammdaten ▸ Bankzugänge ▸ HBCI ▸ HBCI-Bankzugang* erfolgen.

3.6 Schlüssel für weitere Benutzerkennungen verwenden

Nach der Erstellung der Sicherheitsdatei kann der Benutzer bei der Neuanlage von weiteren HBCI-Konten bei diesem Institut (sofern dafür eine andere Benutzerkennung verwendet wird) oder auch für die Konten bei anderen Instituten die gleiche Sicherheitsdatei (für den gleichen Benutzer) verwenden.

Definieren Sie den neuen Benutzer, wie oben beschrieben, und legen Sie den Wechseldatenträger ein bzw. wählen Sie das Verzeichnis aus. Wählen Sie für den Benutzer im Reiter *Sicherheitsmedium* die Schaltfläche <Initialisieren / Freischalten>. Die Datei wird gelesen und die Angaben des Benutzers zur visuellen Kontrolle angezeigt. Wählen Sie die Funktion *Das Medium zusätzlich für obigen Benutzer initialisieren* aus, damit die Benutzerkennung der Schlüsseldatei zugeordnet wird.

Mit <Weiter> werden Sie zur Eingabe des Passwortes aufgefordert, das für die Schlüsseldatei bereits hinterlegt ist. Anschließend werden mit <Weiter> die Benutzerdaten und Schlüssel vom Programm ergänzt und am Bildschirm angezeigt.

Die Initialisierung für das Konto wird wiederum mit <Weiter> angestoßen und der Transfer zum Institut nach den oben beschriebenen Schritten aufgebaut.

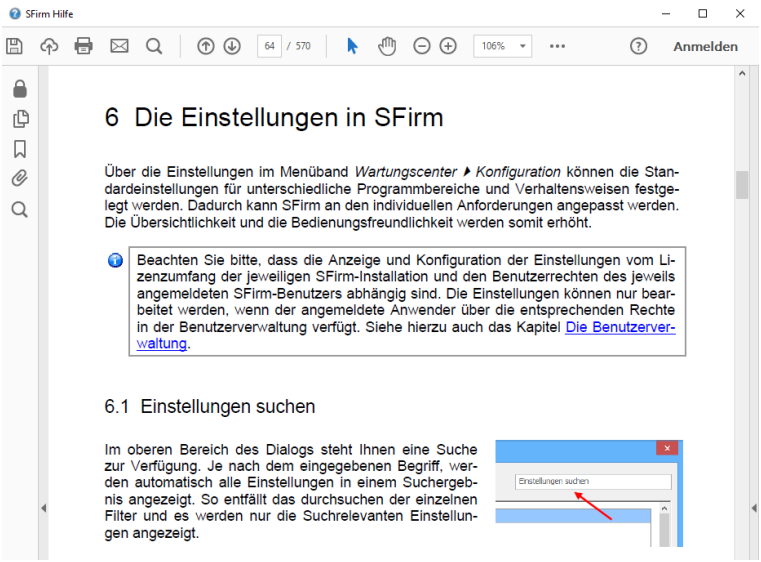
4 Weitere Informationsquellen & Support

Neben dem Kundenhandbuch und den Kundenleitfäden stellen die Hilfe und die Inhalte des Internetauftritts www.sfirm.de weitere Quellen dar, Informationen rund um SFirm zu erhalten. Mit den angebotenen Seminaren haben Sie außerdem die Möglichkeit, themenbezogen das eigene Wissen in Theorie und Praxis zu vertiefen. Zusätzlich dazu hilft Ihnen der technische Kundenservice des Herstellers bei allen technischen Fragen und Problemen. Im letzten Abschnitt finden Sie alle Kontaktdaten im Überblick.

4.1 Die Hilfe in SFirm

Die Hilfe ist ein Bestandteil der Anwendung SFirm. Sie ist mit den jeweiligen Programmteilen bzw. Funktionen verbunden und zeigt Ihnen – je nachdem, wo Sie sich gerade befinden – nach dem Aufruf mit der F1-Taste die entsprechend zugehörige Beschreibung und Hilfe an.

Die Hilfe ist überwiegend nach Programmbereichen und Programmfunktionen strukturiert und gibt Ihnen somit auch die Möglichkeit, sich über diese Hilfe in SFirm einzuarbeiten.

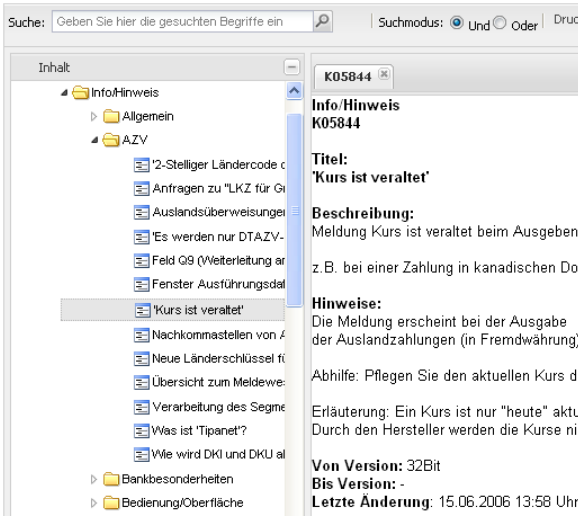


4.2 Der Internetauftritt von SFirm

Über die Adresse www.sfirm.de haben Sie einen Zugang zum SFirm-Internetauftritt. Die SFirm-Website ist in zwei Bereiche eingeteilt: einen allgemein zugänglichen Teil, der auch den Großteil der aktuellen Informationen zu den Produkten und Modulen enthält und einen exklusiven Bereich für die Berater der Sparkassen und Landesbanken. Im öffentlichen Teil sind mehrere Rubriken zu sehen, über die Sie aktuelle Informationen, Leitfäden, Modulbeschreibungen und Schulungsangebote sowie Downloads von Updates und Tools erreichen können.

4.2.1 SFirm-KnowledgeBase

Die SFirm-KnowledgeBase ist eine Wissensdatenbank, die Informationen, Hinweise und Problemlösungen zu den aktuellen, freigegebenen Versionen von SFirm strukturiert zur Verfügung stellt. Der Aufruf der KnowledgeBase erfolgt über die Rubrik *Support ▸ FAQ Hilfedatenbank.*



4.2.2 Seminare

Für SFirm bieten wir Ihnen eine Reihe von Seminaren an, die sich an unterschiedliche Zielgruppen wendet. Eine Auflistung der derzeit angebotenen Seminare erhalten Sie über den SFirm-Internetauftritt www.sfirm.de in der Rubrik *Seminare*. Für nähere Informationen steht Ihnen auch unser Seminar-Team telefonisch und per E-Mail zur Verfügung (siehe übernächsten Abschnitt).

4.3 Der technische Kundenservice

Der Hersteller bietet Ihnen einen kostenpflichtigen technischen Support für alle SFirm-Produkte an. Detaillierte Informationen finden Sie auf der Seite www.sfirm.de in der Rubrik *Kontakt*. Die SFirm-Hotline steht Ihnen von montags - freitags von 8:00 bis 20:00 Uhr unter folgender kostenpflichtigen Rufnummer zur Verfügung:

0900 / 11 55 99 0 (1,99 EUR/Minute inkl. MwSt. aus dem dt. Festnetz; abweichende Preise für Mobilfunkteilnehmer).

4.4 Kontaktinformationen

Folgende Tabelle gibt Ihnen einen Überblick über die wichtigsten Kontaktdaten des Herstellers:

Anschrift		Star Finanz-Software Entwicklung und Vertriebs GmbH Laatzener Straße 5 30539 Hannover
Internetauftritte:	Produktseite Firmenseite	www.sfirm.de www.starfinanz.de
Vertrieb Rufnummer		040 / 23728 - 333
Vertrieb Fax		040 / 23728 - 166
Vertrieb E-Mail		vertrieb@starfinanz.de
Technische Hotline für Endkunden		0900 / 11 55 99 0 (1,99 EUR/Minute inkl. MwSt. aus dem deutschen Festnetz; abweichende Preise für Mobilfunkteilnehmer).