



Kundenleitfaden

Einrichtung HBCI

Finanzen. Professionell. Managen.

5.324,11
3.531,20
523,30
789,31
1.030,50
855,28
10.632,85
479,24
523,30
789,31
1.030,50
855,28
855,28
10.632,85
479,24
24.324,03
807,23
11.478,07
645,13
3.075,33
523,30

Dezember 2024



Inhalt

1 HBCI mit PIN und TAN einrichten.....	4
1.1 Einstieg in die Einrichtung	4
1.2 Assistent zur Einrichtung ausführen	5
1.3 Verfügungsberechtigte / Rundrufdefinition	6
1.4 Weitere Verfahren bzw. Wechsel zwischen den TAN-Verfahren	7
1.4.1 chipTAN (manuell/optisch/QR).....	8
1.4.2 chipTAN USB	11
1.4.3 Zwangsänderung der Start-PIN mit chipTAN	12
1.4.4 pushTAN / pushTAN 2.0	13
1.4.5 smsTAN.....	14
1.4.6 Automatischer Medienbezeichnungswechsel (smsTAN/pushTAN)	17
1.4.7 PIN im HBCI-Bankzugang hinterlegen	17
1.4.8 PIN beim Abholen oder Senden hinterlegen	18
1.4.9 Hinterlegte PIN ändern oder löschen	18
2 HBCI mit Chipkarte einrichten	19
2.1 Voraussetzungen zu HBCI mit Chipkarte	19
2.2 HBCI mit einer DDV-Chipkarte konfigurieren.....	19
2.2.1 Neuanlage eines Kontos per HBCI	20
2.2.2 HBCI für ein bestehendes Konto einrichten	22
2.3 HBCI mit einer RAH-Chipkarte konfigurieren.....	24
2.3.2 Neuanlage eines Kontos HBCI-Kontos mit einem RAH-7 Medium.....	24
2.4 Kontoanlage mit einer RDH-Chipkarte	27
2.4.1 Kontoanlage mit einer vorgelegten RDH-Karte	27
2.4.2 Kontoanlage mit einer leeren RDH-Karte.....	29
2.4.3 Einrichtung mit einer SECCOS-Karte.....	33
2.5 Pin/Passwort verwalten (HBCI)	36
2.6 Kartenleser einstellen.....	36
2.6.2 Kartenleser in Remotedesktopserver-Umgebungen.....	39
3 HBCI mit Sicherheitsdatei einrichten	42
3.1 Voraussetzungen	42
3.2 Erfassung einer Kontoverbindung	42
3.3 Der Assistent zur manuellen Konfiguration.....	42
3.4 Einen Benutzer anlegen	43
3.5 Initialisieren und Freischalten	44
3.6 Schlüssel für weitere Benutzerkennungen verwenden	45
4 Weitere Informationsquellen & Support.....	46
4.1 Die Hilfe in SFirm	46
4.2 Der Internetauftritt von SFirm	46
4.2.1 SFirm Hilfe-Center.....	47
4.2.2 Seminare	47
4.3 Der technische Kundenservice.....	47
4.4 Kontaktinformationen	48

Copyrights und Warenzeichen

Windows, Windows Server, SQL Server und Hyper-V sind eingetragene Warenzeichen der Microsoft Corp. Alle in dieser Dokumentation zusätzlich verwendeten Programmnamen und Bezeichnungen sind u.U. ebenfalls eingetragene Warenzeichen der Herstellerfirmen und dürfen nicht gewerblich oder in sonstiger Weise verwendet werden. Irrtümer vorbehalten.

Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt gearbeitet. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Die angegebenen Daten dienen lediglich der Produktbeschreibung und sind nicht als zugesicherte Eigenschaft im Rechtssinne zu verstehen.

Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder juristische Verantwortlichkeit noch irgendeine Haftung übernehmen. Alle Rechte vorbehalten; kein Teil dieser Dokumentation darf in irgendeiner Form (Druck, Fotokopie oder die Speicherung und/oder Verbreitung in elektronischer Form) ohne schriftliche Genehmigung der Star Finanz-Software Entwicklung und Vertriebs GmbH reproduziert oder vervielfältigt werden.

Die Star Finanz entwickelt ihre Produkte ständig weiter, um Ihnen den größtmöglichen Komfort zu bieten. Deshalb bitten wir um Verständnis dafür, dass sich Abweichungen vom Handbuch zum Produkt ergeben können.



Copyright © 1999-2024

Star Finanz-Software Entwicklung und Vertriebs GmbH - Grüner Deich 15 - 20097 Hamburg.

1 HBCI mit PIN und TAN einrichten

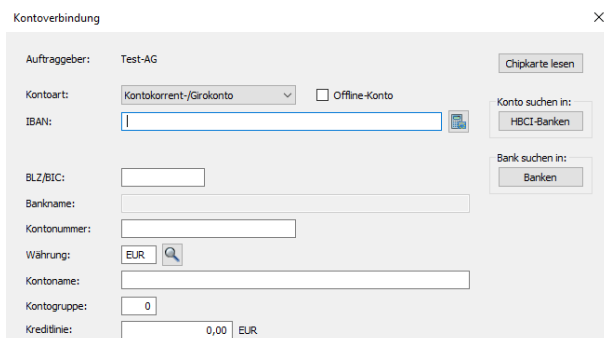
Um einen Datentransfer per HBCI (Homebanking Computer Interface) durchführen zu können, muss die Kontoverbindung zunächst für diesen Übertragungsweg konfiguriert werden. Die derzeit von SFirm unterstützten HBCI-Verfahrensweisen sind die per *PIN/TAN*, per *Sicherheitsdatei* und per Chipkarte.

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.

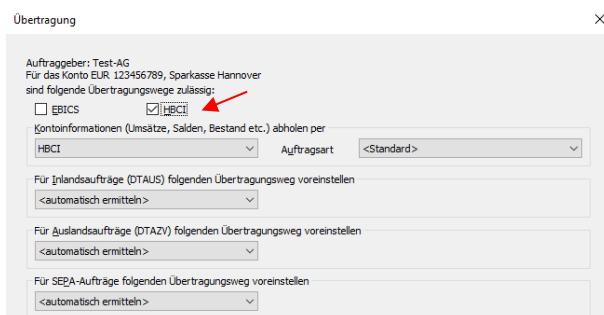
-  Die Konfiguration des Übertragungsweges für HBCI mit PIN/TAN wird in dem Kapitel **Übertragungswege einstellen** beschrieben und wird hier vorausgesetzt.
-  Wenn hier von Benutzerkennung gesprochen wird, handelt es sich um den technischen Begriff. Die Banken verwenden dafür oft Marketingnamen, wie Legitimations-ID, VRNetKey oder Postbank-ID. In jedem Fall handelt es sich um den Anmeldename am Bankrechner.

1.1 Einstieg in die Einrichtung

Die Neuanlage eines Kontos wird im Dialog *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 vorgelegt. 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>.

HBCI einrichten

Um für dieses Konto HBCI zu konfigurieren, wählen Sie einen der folgenden Punkte

☐ HBCI mit Chipkarte

Wenn Ihnen von Ihrem Kreditinstitut eine Chipkarte ausgehändigt wurde, wählen Sie bitte diesen Punkt.

☐ HBCI mit PIN und TAN

Haben Sie von Ihrem Kreditinstitut eine PIN und eine TAN-Liste, einen TAN-Generator erhalten oder nutzen Sie das smsTAN/mobileTAN-Verfahren, wählen Sie diesen Punkt.

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.

HBCI PIN/TAN einrichten

Für den Kontozugang mittels HBCI PIN/TAN wird ein HBCI-Benutzer benötigt. Ein HBCI-Benutzer identifiziert sich gegenüber des Kreditinstitutes mit seiner Benutzerkennung und evtl. seiner Kunden-ID. Dieser Dialog soll Sie bei der Anlage eines HBCI-Benutzers unterstützen.

☒ Kontonummer als HBCI-Benutzerkennung verwenden

Kreditinstitut: Sparkasse Hannover (BLZ 25050180) verwendet für die HBCI PIN/TAN Anmeldung in der Regel die Kontonummer des ersten Kontos (bzw. Hauptkontos) bei diesem Kreditinstitut. Bitte wählen Sie das entsprechende Konto aus.

123456789 (EUR 123456789, Sparkasse Hannover)

Bei den Verfahren...

- pushTAN / pushTAN 2.0 (decoupled)
- chipTAN (manuell/optisch/USB/QR)
- SmartTAN
- smsTAN
- photoTAN

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

☒ HBCI-Anmeldedaten selbst eintragen

Falls Ihnen von Ihrem Kreditinstitut eine spezielle HBCI PIN/TAN Benutzerkennung zugewiesen wurde oder Sie selbst eine eingerichtet haben, können Sie diese hier eingeben.

Legitimations-ID (techn.: HBCI-Benutzerkennung)

Tester

Kunden-ID (wird bei diesem Institut automatisch gefüllt)

Zugeordneter SFirm-Benutzer (wird zur Prüfung der Kontoberechtigungen benötigt)


MUSTERMANN



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.

 Ihr Kreditinstitut unterstützt neben HBCI Version 2.2 auch Version 3.0. Da SFirm automatisch die aktuellere HBCI Version verwenden wird, ist es empfehlenswert, auch die Bank- und Benutzerdaten für diese Version abzuholen.

Möchten Sie jetzt Bank- und Benutzerdaten für HBCI 3.0 von Ihrem Kreditinstitut abholen?

Ja Nein

1.3 Verfügbare Berechtigungen / Rundrufdefinition

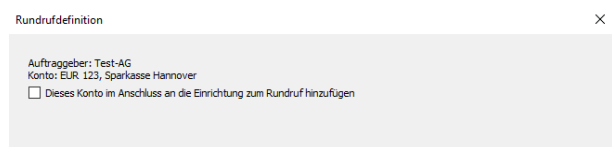
Nachdem die Daten erfolgreich transferiert wurden, erscheint eine Abfrage, ob für dieses Konto weitere HBCI-Benutzer eingerichtet werden sollen.

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 *Rundrufdefinition* 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 entsprechenden Sicherheitsmedium und der Benutzerkennung angezeigt.

Verbindungsdaten Benutzer Geschäftsvorfälle Sonstiges					
Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser zu gruppieren					
Status	Interner Name	Sicherheits...	Benutzerkenn...	Kunden-ID	berech...
▼					
▶	Initialisiert	MUSTERMANN	PIN-TAN	123456789	123456789 Nein

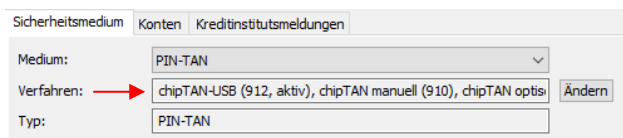
1.4 Weitere Verfahren bzw. Wechsel zwischen den TAN-Verfahren

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

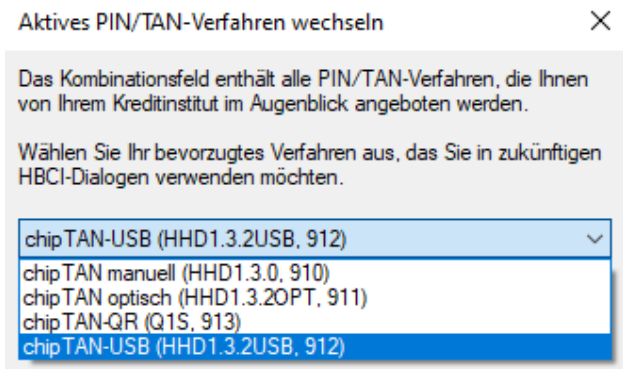
- pushTAN /pushTAN 2.0 (decoupled)
- chipTAN (manuell/optisch/USB/QR)
- SmartTAN
- smsTAN
- photoTAN


vorgenommen werden, markieren Sie im Reiter *Benutzer* den neuen 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...

- pushTAN /pushTAN 2.0 (decoupled)
- smsTAN
- photoTAN

ist damit abgeschlossen. Zum Abschluss der Verfahren...

- chipTAN (manuell/optisch/USB/QR)
- SmartTAN

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

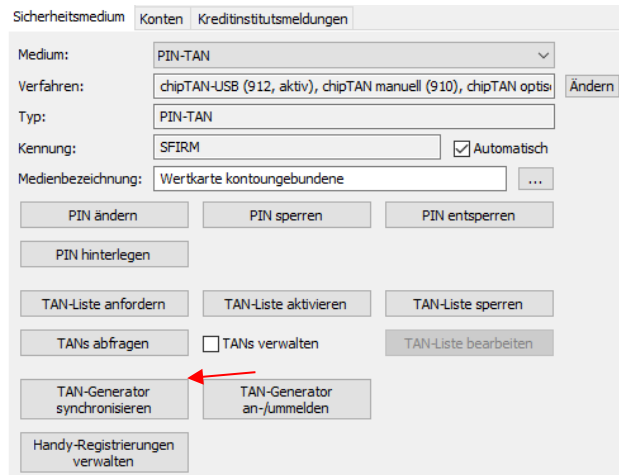
1.4.1 chipTAN (manuell/optisch/QR)

1.4.1.1 TAN-Generator synchronisieren

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

- chipTAN
- SmartTAN

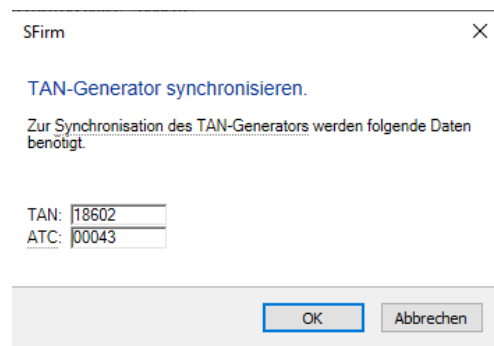
der TAN-Generator synchronisiert werden (Schaltfläche *TAN-Generator synchronisieren*).




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 Kartenummer 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.

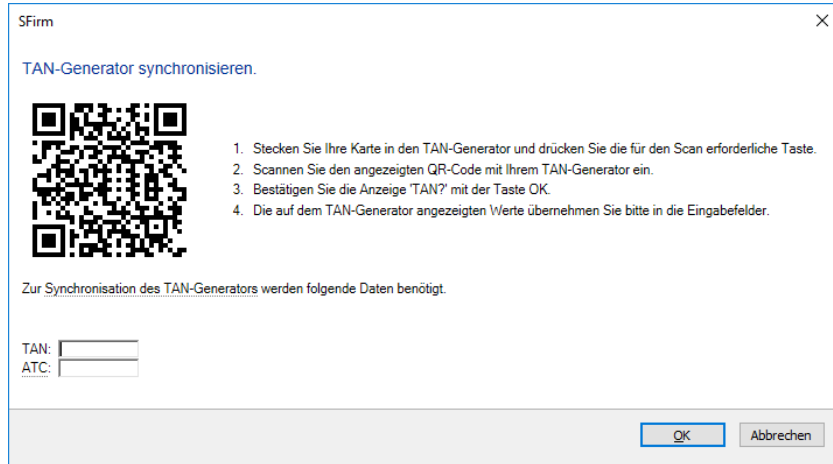
Liegen mehrere Karten vor, können Sie die entsprechende anschließend über das Auswahlfeld selektieren (haben Sie die Kartenummer manuell eingegeben, steht dieses Auswahlfeld nicht zur Verfügung). Ermitteln Sie anschließend die ATC der Chipkarte über den TAN-Generator.




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

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

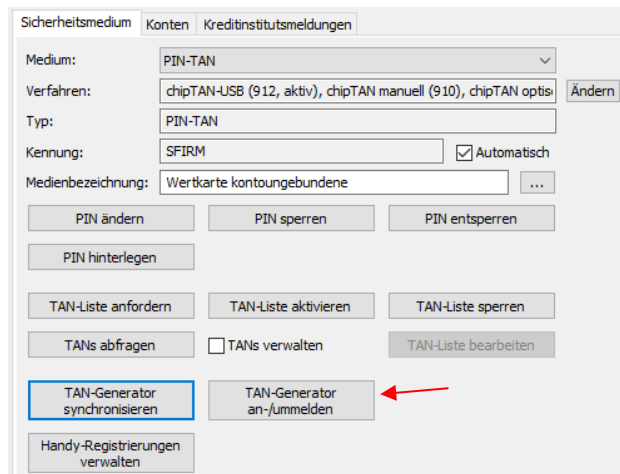
Wenn Sie chipTAN QR verwenden, erscheint ein entsprechend für das Verfahren angepasster Dialog, der Ihnen wichtige Hinweise auf die durchzuführenden Schritte gibt.



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 Kartenummer die Kartenummer 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.

SFirm

×

TAN-Generator an-/ummelden.

Zum An-/Ummelden des TAN-Generators bzw. Ihrer Karte werden folgende Daten benötigt.

Kartennummer:

[Verfügbare Karten ermitteln.](#)

TAN:

ATC:

OK


Abbrechen

Bei dem Verfahren chipTAN QR wird auch bei dieser Aktion der QR-Code und die Hinweise angezeigt.

SFirm

×

TAN-Generator an-/ummelden.



1. Stecken Sie Ihre Karte in den TAN-Generator und drücken Sie die für den Scan erforderliche Taste.
2. Scannen Sie den angezeigten QR-Code mit Ihrem TAN-Generator ein.
3. Bestätigen Sie die Anzeige 'TAN?' mit der Taste OK.
4. Die auf dem TAN-Generator angezeigten Werte übernehmen Sie bitte in die Eingabefelder.

Zum An-/Ummelden des TAN-Generators bzw. Ihrer Karte werden folgende Daten benötigt.

Kartennummer:

[Verfügbare Karten ermitteln.](#)

TAN:

ATC:

OK

Abbrechen



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.

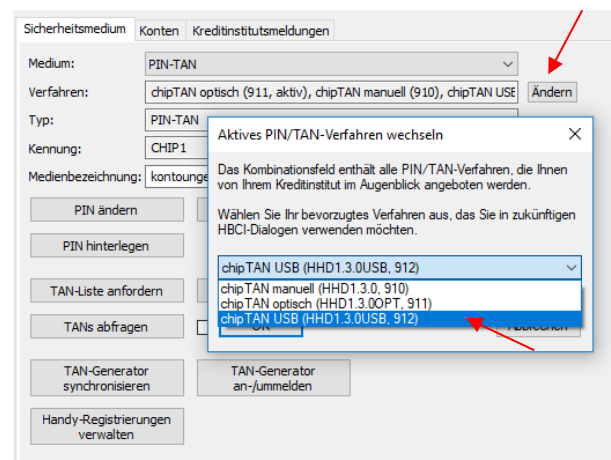
- Wenn Sie bei Ihrem Institut das chipTAN-/SmartTAN-Verfahren bereits nutzen, können Sie das Verfahren ebenfalls als chipTAN USB nutzen, sobald ein entsprechender Kartenleser angeschlossen ist.

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

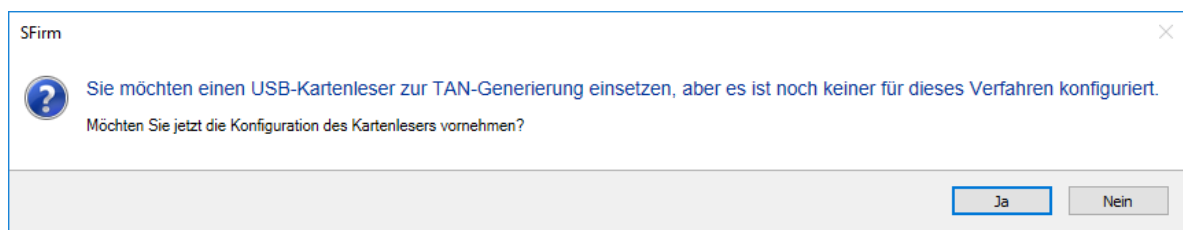
1.4.2.2 Verfahren wählen

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>

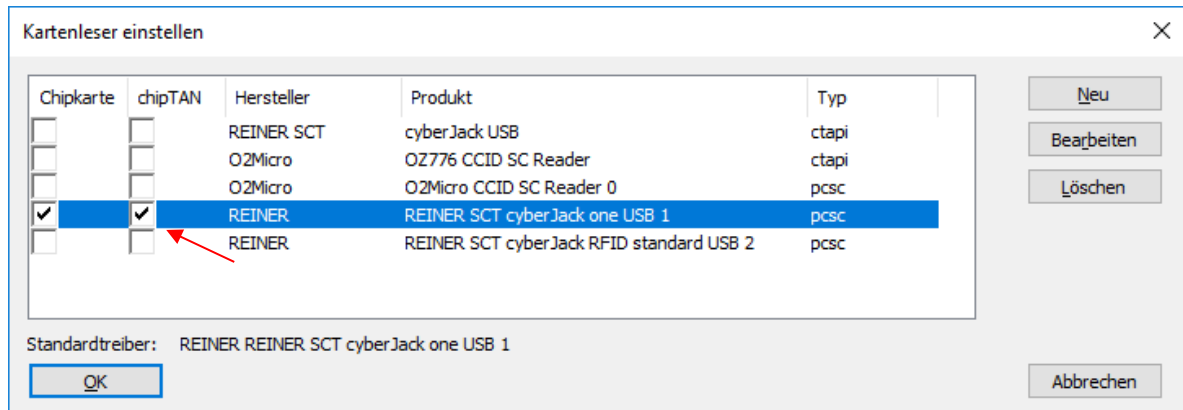


Anschließend prüft SFirm, ob ein geeigneter Kartenleser angeschlossen und verfügbar ist. Wenn das nicht der Fall sein sollte, erscheint die folgende Meldung:



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 cyberJack 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 Zwangsänderung der Start-PIN mit chipTAN

Wenn noch kein aktiver Banking-Zugang besteht, muss vor der Erstverwendung die Start-PIN geändert werden. Dies kann entweder über das Internet-Banking des Instituts oder aber direkt in SFirm durchgeführt werden. Wird mit dem chipTAN-Verfahren (manuell/optisch/QR) gearbeitet, ist ein bestimmtes Vorgehen zu beachten:

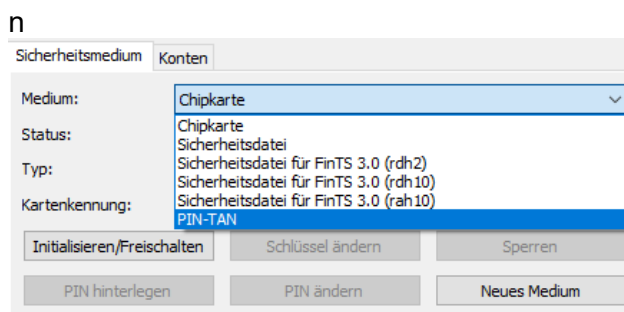
1. HBCI-Bankzugang und HBCI-Benutzer einrichten
2. Zugang synchronisieren
3. Bei der nachfolgenden Nachfrage bzgl. PIN-Änderung, eine neue PIN vergeben und mit einer TAN bestätigen

Um die TAN zu erzeugen muss das Lesegerät in den ATC-Modus versetzt werden. Bei Lesegeräten von Reiner-SCT halten Sie bei eingeführter Chipkarte die TAN-Taste (@-Taste) so lange gedrückt, bis *ATC Anzeige aktiviert* im Display erscheint, anschließend wird *Start-Code* angezeigt. Drücken Sie jetzt einmal die TAN-Taste. Es wird Ihnen nun neben dem ATC auch die TAN angezeigt.

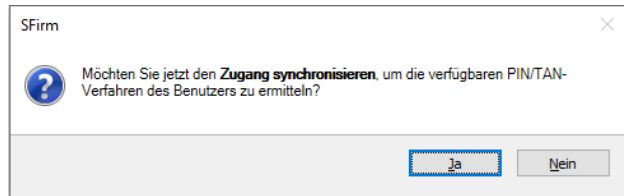
1.4.4 pushTAN / pushTAN 2.0

Um das pushTAN Verfahren nutzen zu können, ist eine Freischaltung des Verfahrens bei Ihrem Institut erforderlich. Bei diesem Verfahren wird Ihnen die TAN über eine App auf Ihr Handy übermittelt. Da sich die Einrichtung dieser App von Institut zu Institut unterscheiden kann, wenden Sie sich diesbezüglich bitte zur Unterstützung an Ihren Berater des jeweiligen Instituts.

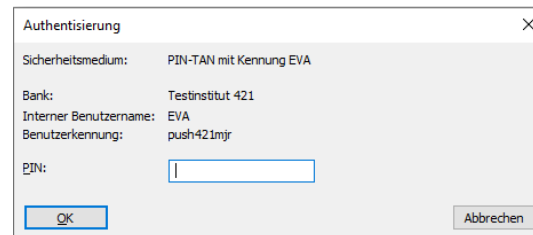
Für das Anlegen eines HBCI-Benutzers, der für das pushTAN Verfahren freigeschaltet ist, geben Sie die entsprechenden Benutzerdaten ein und wählen Sie als Medium PIN-TAN



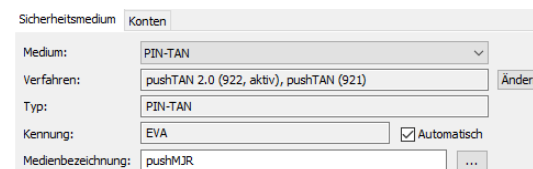
Anschließend erhalten Sie die nebenstehende Meldung. Bestätigen Sie diese mit <JA>.



Um den HBCI-Benutzer zu synchronisieren werden Sie aufgefordert Ihre PIN einzugeben. Geben Sie Ihre PIN ein und bestätigen Sie mit der Schaltfläche <OK>. Die für diesen HBCI-Benutzer verfügbaren PIN/TAN Verfahren werden vom Institut abgefragt.



Im Anschluss wird Ihnen im Feld *Verfahren* angezeigt, welches TAN verfahren aktiv ist und ob weitere zur Verfügung stehen. Daneben befindet sich die Schaltfläche <Ändern>, mit der Sie das aktive TAN Verfahren wechseln können.



1.4.5 smsTAN

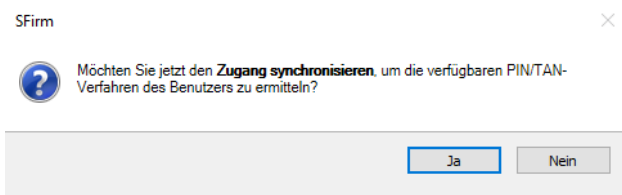
Für das Anlegen eines HBCI-Benutzers, der für das smsTAN freigeschaltet ist, geben Sie die entsprechenden Benutzerdaten ein und klicken im Einrichtungsdialog auf <OK>. Anschließend erhalten Sie die nebenstehende Meldung.

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.

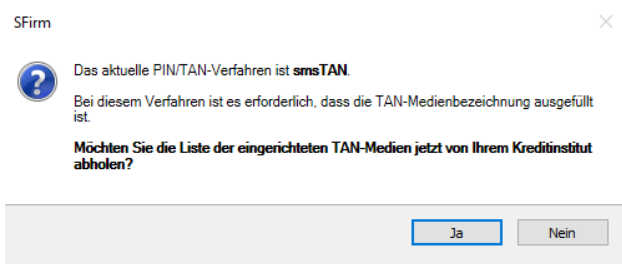
Nur wenn mehrere TAN-Medien vorliegen, erhalten Sie nebenstehende Meldung. Wählen Sie hier die zu verwendende Bezeichnung aus und bestätigen Sie die Auswahl mit <OK>.

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



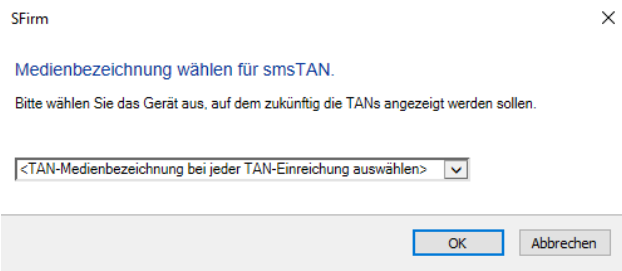
SFirm

Möchten Sie jetzt den **Zugang synchronisieren**, um die verfügbaren PIN/TAN-Verfahren des Benutzers zu ermitteln?



SFirm

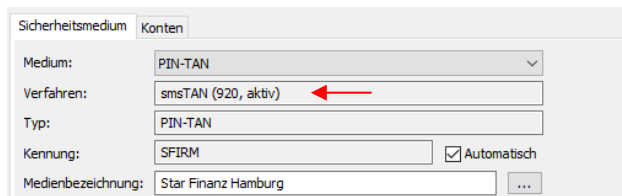
Das aktuelle PIN/TAN-Verfahren ist **smsTAN**.
Bei diesem Verfahren ist es erforderlich, dass die TAN-Medienbezeichnung ausgefüllt ist.
Möchten Sie die Liste der eingerichteten TAN-Medien jetzt von Ihrem Kreditinstitut abholen?



SFirm

Medienbezeichnung wählen für smsTAN.
Bitte wählen Sie das Gerät aus, auf dem zukünftig die TANs angezeigt werden sollen.

<TAN-Medienbezeichnung bei jeder TAN-Einreichung auswählen> ▼



Sicherheitsmedium Konten

Medium: PIN-TAN ▼

Verfahren: smsTAN (920, aktiv) ←

Typ: PIN-TAN

Kenntung: SFIRM ☒ Automatisch

Medienbezeichnung: Star Finanz Hamburg ...

1.4.5.1 Handy-Registrierungen verwalten (smsTAN)

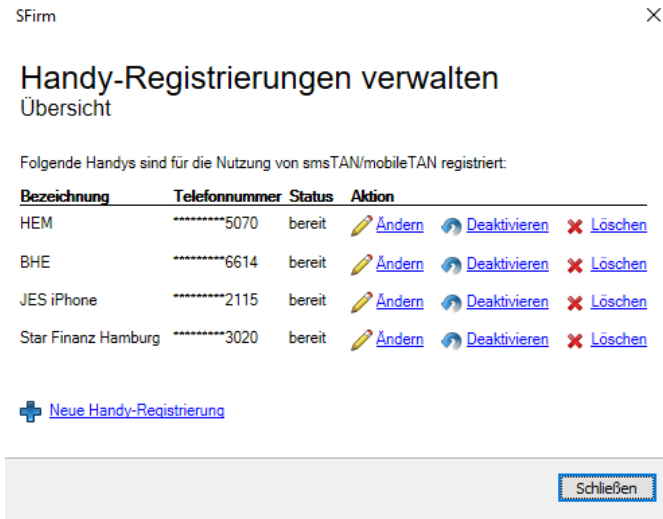
Hier haben Sie die Möglichkeit, Handy-Registrierungen zu verwalten. Nach der Eingabe Ihrer PIN werden die hinterlegten Registrierungen vom Kreditinstitut abgeholt.



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.



Handy-Registrierungen verwalten Übersicht

Folgende Handys sind für die Nutzung von smsTAN/mobileTAN registriert:

Bezeichnung	Telefonnummer	Status	Aktion
HEM	*****5070	bereit	Ändern Deaktivieren Löschen
BHE	*****6614	bereit	Ändern Deaktivieren Löschen
JES iPhone	*****2115	bereit	Ändern Deaktivieren Löschen
Star Finanz Hamburg	*****3020	bereit	Ändern Deaktivieren Löschen

[+ Neue Handy-Registrierung](#)

[Schließen](#)

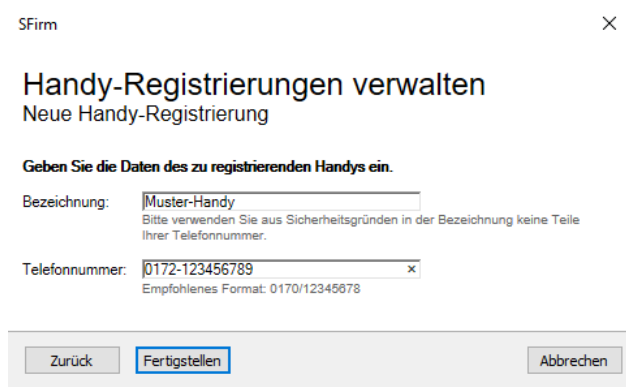
Mobilfunkverbindung registrieren

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.



Handy-Registrierungen verwalten Neue Handy-Registrierung

Geben Sie die Daten des zu registrierenden Handys ein.

Bezeichnung:
Bitte verwenden Sie aus Sicherheitsgründen in der Bezeichnung keine Teile Ihrer Telefonnummer.

Telefonnummer:
Empfohlenes Format: 0170/12345678

[Zurück](#) [Fertigstellen](#) [Abbrechen](#)



Handy-Registrierungen verwalten Neue Handy-Registrierung

✓ Die Handy-Registrierung wurde erfolgreich durchgeführt.

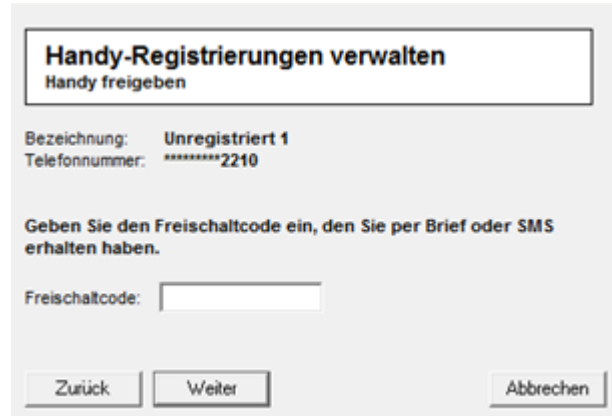
Falls dies Ihre erste Handy-Registrierung bei Ihrem Kreditinstitut ist, erhalten Sie in einigen Tagen einen Registrierungsbrief per Post. Darin wird Ihnen ein Freischaltcode mitgeteilt, mit dem Sie über den "Freigeben"-Link auf der Übersichtsseite das Handy für die Nutzung per smsTAN/mobileTAN freischalten können.

[OK](#)

Mobilfunkverbindung freischalten

Sollte bei einer Telefonnummer die Aktion <Freigegeben> 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.



Handy-Registrierungen verwalten
Handy freigegeben

Bezeichnung: Unregistriert 1
Telefonnummer: *****2210

Geben Sie den Freischaltcode ein, den Sie per Brief oder SMS erhalten haben.

Freischaltcode:

Zurück Weiter Abbrechen

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.



Handy-Registrierungen verwalten
Handy-Registrierung ändern

Bezeichnung: HTC
Telefonnummer: *****3740

Geben Sie die neuen Daten Ihres Handys ein.

Bezeichnung: HTC
Bitte verwenden Sie aus Sicherheitsgründen in der Bezeichnung keine Teile Ihrer Telefonnummer.

Telefonnummer:
Wenn Sie keine Änderung der Telefonnummer vornehmen möchten, lassen Sie das Eingabefeld einfach leer.

Zurück Fertigstellen Abbrechen

Mobilfunkverbindung deaktivieren/löschen

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



Handy-Registrierungen verwalten
Handy deaktivieren

Bezeichnung: HTC
Telefonnummer: *****3740

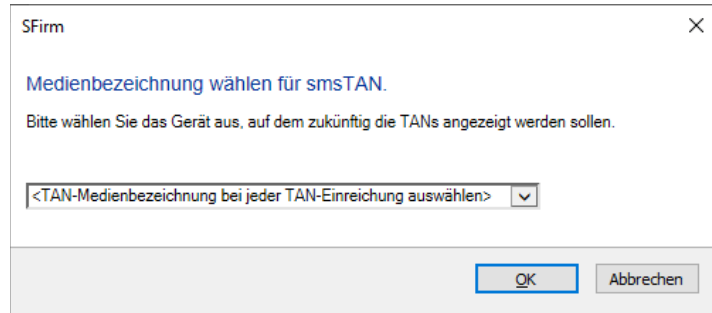
Klicken Sie auf "Fertigstellen", um das angegebene Handy zu deaktivieren.

Zurück Fertigstellen Abbrechen

1.4.6 Automatischer Medienbezeichnungswechsel (smsTAN/pushTAN)

Ein Benutzer, der smsTAN oder pushTAN verwendet, wechselt sein Smartphone. Beim nächsten TAN-pflichtigen Auftrag bekommt der Benutzer vom Rechenzentrum eine Rückmeldung, dass die TAN-Medienbezeichnung falsch oder ungültig sei (HBCI-Codes: 9955 und 9962), worauf SFirm automatisch eine Aufforderung einblendet, eine neue Liste der eingereichten TAN-Medien abzuholen bzw. ein neues TAN-Medium zu wählen.

Bei einer fehlenden TAN-Bezeichnung im HBCI-Benutzer, wird SFirm das Fenster TAN-Medienbezeichnung öffnen, um eine TAN-Medienbezeichnung für diesen Auftrag zu verwenden bzw. dauerhaft für den HBCI-Benutzer zu speichern, wenn in SFirm eine Liste der TAN-Medien bereit steht. Ansonsten erscheint zunächst eine Aufforderung die Liste der TAN-Medien neu abzuholen.



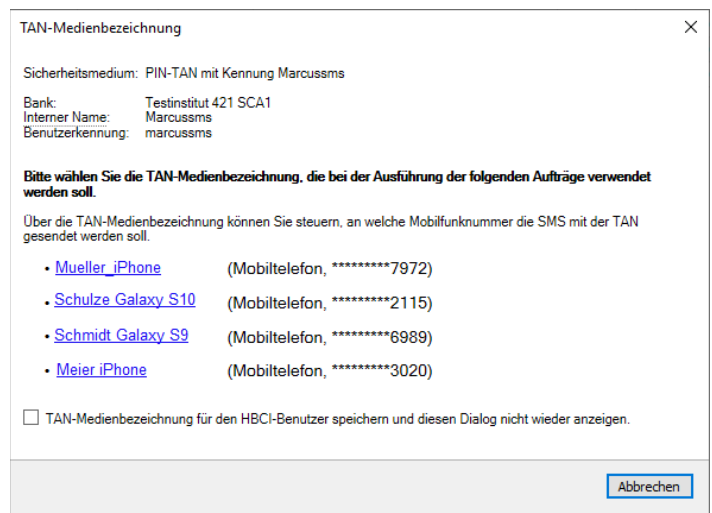
SFirm

Medienbezeichnung wählen für smsTAN.

Bitte wählen Sie das Gerät aus, auf dem zukünftig die TANs angezeigt werden sollen.

<TAN-Medienbezeichnung bei jeder TAN-Einreichung auswählen>

OK Abbrechen



TAN-Medienbezeichnung

Sicherheitsmedium: PIN-TAN mit Kennung Marcussms

Bank: Testinstitut 421 SCA1
 Interner Name: Marcussms
 Benutzerkennung: marcussms

Bitte wählen Sie die TAN-Medienbezeichnung, die bei der Ausführung der folgenden Aufträge verwendet werden soll.

Über die TAN-Medienbezeichnung können Sie steuern, an welche Mobilfunknummer die SMS mit der TAN gesendet werden soll.

- [Mueller iPhone](#) (Mobiltelefon, *****7972)
- [Schulze Galaxy S10](#) (Mobiltelefon, *****2115)
- [Schmidt Galaxy S9](#) (Mobiltelefon, *****6989)
- [Meier iPhone](#) (Mobiltelefon, *****3020)

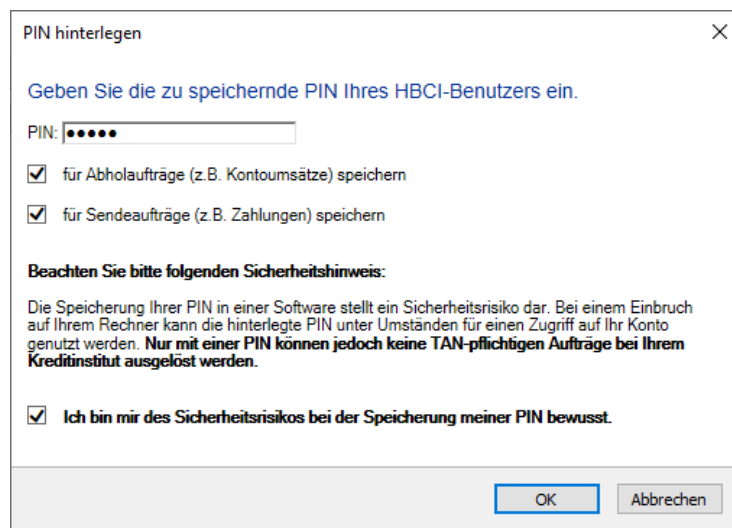
☐ TAN-Medienbezeichnung für den HBCI-Benutzer speichern und diesen Dialog nicht wieder anzeigen.

Abbrechen

1.4.7 PIN im HBCI-Bankzugang hinterlegen

Im HBCI-Bankzugang kann pro hinterlegten Benutzer die PIN über die Schaltfläche <PIN hinterlegen> in SFirm gespeichert werden. Dabei werden Abholaufträge und Sendeaufträge gesondert betrachtet.

Die Speicherung Ihrer PIN in einer Software stellt ein Sicherheitsrisiko dar. Bei einem Einbruch auf Ihrem Rechner kann die hinterlegte PIN unter Umständen für einen Zugriff auf Ihr Konto genutzt werden.



PIN hinterlegen

Geben Sie die zu speichernde PIN Ihres HBCI-Benutzers ein.

PIN: [.....]

☒ für Abholaufträge (z.B. Kontoumsätze) speichern

☒ für Sendeaufträge (z.B. Zahlungen) speichern

Beachten Sie bitte folgenden Sicherheitshinweis:

Die Speicherung Ihrer PIN in einer Software stellt ein Sicherheitsrisiko dar. Bei einem Einbruch auf Ihrem Rechner kann die hinterlegte PIN unter Umständen für einen Zugriff auf Ihr Konto genutzt werden. **Nur mit einer PIN können jedoch keine TAN-pflichtigen Aufträge bei Ihrem Kreditinstitut ausgelöst werden.**

☒ Ich bin mir des Sicherheitsrisikos bei der Speicherung meiner PIN bewusst.

OK Abbrechen

1.4.8 PIN beim Abholen oder Senden hinterlegen

Beim manuellen Abholen (z.B. von Kontoumsätzen) wird Ihnen angeboten die PIN zu hinterlegen, wenn noch keine PIN hinterlegt ist.

Die Speicherung Ihrer PIN in einer Software stellt ein Sicherheitsrisiko dar. Bei einem Einbruch auf Ihrem Rechner kann die hinterlegte PIN unter Umständen für einen Zugriff auf Ihr Konto genutzt werden.

Autorisation für Konto EUR 32508814

Sicherheitsmedium:

HBCI PIN/TAN

Bank:

Testinstitut 421 SCA1

Interner Benutzername:

SFIRM

Benutzerkennung:

mira | 2.TAN-Liste

PIN

•••••

☒ PIN speichern (für Abholaufträge, z.B. Kontoumsätze)

Beachten Sie bitte folgenden Sicherheitshinweis:
 Die Speicherung Ihrer PIN in einer Software stellt ein Sicherheitsrisiko dar. Bei einem Einbruch auf Ihrem Rechner kann die hinterlegte PIN unter Umständen für einen Zugriff auf Ihr Konto genutzt werden.
Nur mit einer PIN können jedoch keine TAN-pflichtigen Aufträge bei Ihrem Kreditinstitut ausgelöst werden.

Weiter

Abbrechen

Beim manuellen Senden (z.B. Ausgeben von Überweisungen) wird Ihnen angeboten die PIN zu hinterlegen, wenn noch keine PIN hinterlegt ist.

Die Speicherung Ihrer PIN in einer Software stellt ein Sicherheitsrisiko dar. Bei einem Einbruch auf Ihrem Rechner kann die hinterlegte PIN unter Umständen für einen Zugriff auf Ihr Konto genutzt werden.

Autorisation des Auftrags

Sicherheitsmedium:

HBCI PIN/TAN

Bank:

Testinstitut 421 SCA1

Interner Benutzername:

TRAINER

Benutzerkennung:

MERANO

PIN

•••••

☒ PIN speichern (für Sendeaufträge, z.B. Zahlungen)

Beachten Sie bitte folgenden Sicherheitshinweis:
 Die Speicherung Ihrer PIN in einer Software stellt ein Sicherheitsrisiko dar. Bei einem Einbruch auf Ihrem Rechner kann die hinterlegte PIN unter Umständen für einen Zugriff auf Ihr Konto genutzt werden.
Nur mit einer PIN können jedoch keine TAN-pflichtigen Aufträge bei Ihrem Kreditinstitut ausgelöst werden.

Weiter

Abbrechen

 Nur mit einer PIN können jedoch keine TAN-pflichtigen Aufträge bei Ihrem Kreditinstitut ausgelöst werden.

1.4.9 Hinterlegte PIN ändern oder löschen

Das Löschen und Ändern einer hinterlegten PIN kann nur über den Bankzugang pro Benutzer über die Schaltfläche <PIN hinterlegen> erfolgen.

PIN hinterlegen

Es ist bereits eine PIN hinterlegt.

Sie haben folgende Möglichkeiten:

- hinterlegte PIN [ändern](#)
- hinterlegte PIN [löschen](#)

Abbrechen

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 muss 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

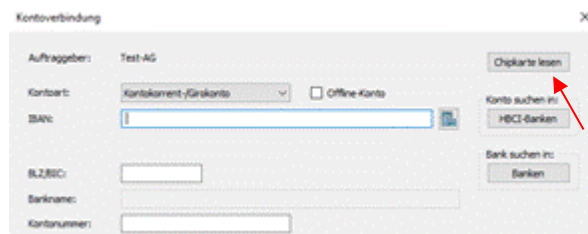
In diesem Abschnitt wird die Einrichtung von HBCI für das Medium Chipkarte beschrieben, zunächst aber ausschließlich für den Chipkarten-Typ DDV (der fast ausschließlich von den Sparkassen/Landesbanken eingesetzt wird). Die Konfiguration eines Kontos für HBCI mit Chipkarte kann – je nach vorliegender 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 <i>Stammdaten</i> ▶ <i>Auftraggeber</i> , 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 <i>Stammdaten</i> ▶ <i>Auftraggeber</i> vorhanden ist und dieses nun dem Übertragungsweg <i>HBCI</i> 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

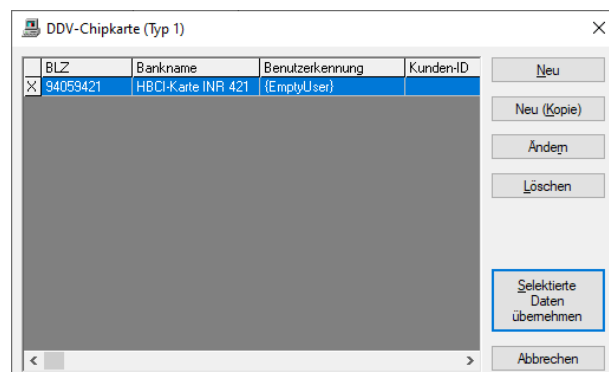
Die hier beschriebene Variante ein Konto für HBCI einzurichten gehört zu der Gängigsten und ist auch die empfohlene. Durch eine strukturierte Abfolge von Dialogen werden das Auftraggeberkonto, der HBCI-Bankzugang, das HBCI-Konto und der HBCI-Teilnehmer „in einem Rutsch“ angelegt. Im Regelfall ist damit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

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

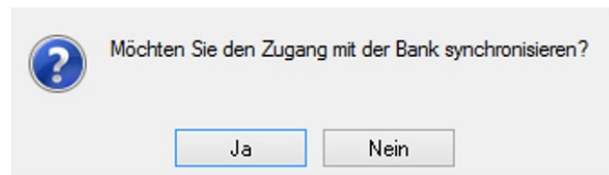



Dieser Dialog kann nachträglich über die Schaltfläche <Neu> bzw. <Ändern> in dem Reiter *Bankkonten* des Dialogs *Auftraggeber* aufgerufen werden.

Die auf der Karte befindlichen und für die Anzeige erforderlichen Daten werden ausgelesen und in dem Fenster *DDV-Chipkarte (Typ 1)* angezeigt. Sind mehrere Einträge (Zeilen) vorhanden, markieren Sie den gewünschten und klicken Sie anschließend auf die Schaltfläche <Selektierte Daten übernehmen>.

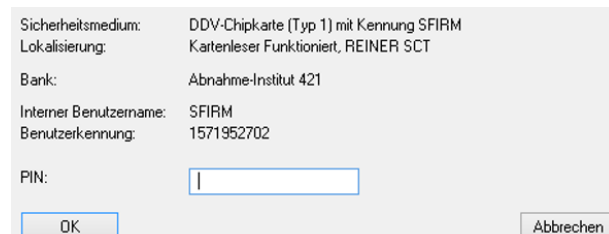


Sie werden anschließend gefragt, ob Sie den Zugang mit der Bank synchronisieren möchten.

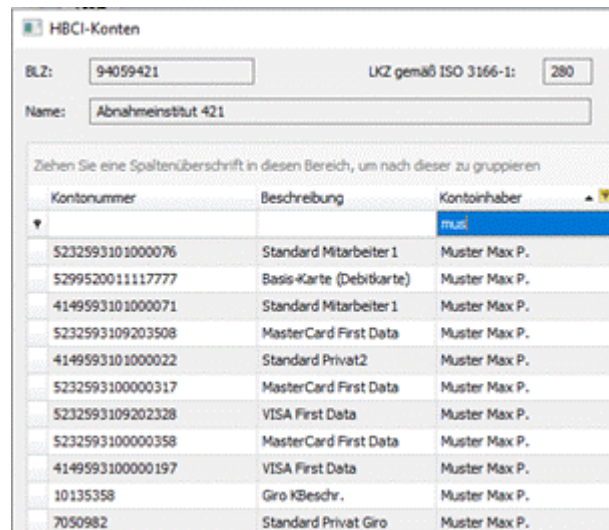


Bestätigen Sie bitte die Meldung mit <Ja>. Die Internetverbindung wird anschließend überprüft und die Dialoginitialisierung durchgeführt.

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.

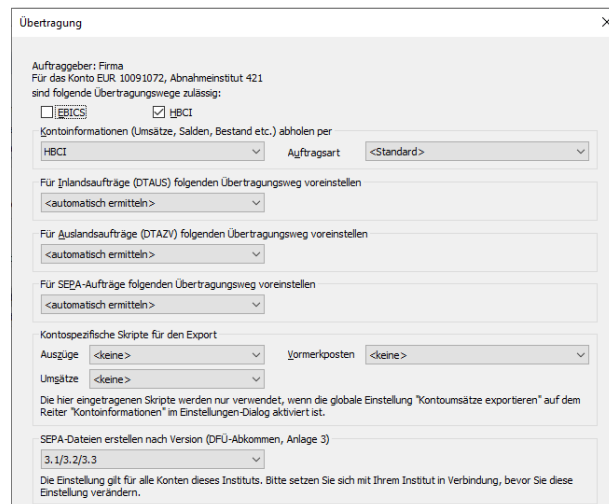


Nach einem erfolgreichen Transfer wird die HBCI-Kommunikation beendet und es erscheint eine Auswahl der verfügbaren Konten des Karteninhabers für dieses Institut in dem Dialog *HBCI Konten*.



Kontonummer	Beschreibung	Kontoinhaber
5232593101000076	Standard Mitarbeiter 1	Muster Max P.
5299520011117777	Basis-Karte (Debitkarte)	Muster Max P.
4149593101000071	Standard Mitarbeiter 1	Muster Max P.
5232593109203508	MasterCard First Data	Muster Max P.
4149593101000022	Standard Privat2	Muster Max P.
5232593100000317	MasterCard First Data	Muster Max P.
5232593109202328	VISA First Data	Muster Max P.
5232593100000358	MasterCard First Data	Muster Max P.
4149593100000197	VISA First Data	Muster Max P.
10135358	Giro KBeschr.	Muster Max P.
7050982	Standard Privat Giro	Muster Max P.

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.



Auftraggeber: Firma
Für das Konto EUR 10091072, Abnahmeinstitut 421
sind folgende Übertragungswege zulässig:

☐ EBICS ☒ HBCI

Kontoinformationen (Umsätze, Salden, Bestand etc.) abholen per
HBCI Auftragsart: <Standard>

Für Inlandsaufträge (DTAUS) folgenden Übertragungsweg voreinstellen
<automatisch ermitteln>

Für Auslandsaufträge (DTAZV) folgenden Übertragungsweg voreinstellen
<automatisch ermitteln>

Für SEPA-Aufträge folgenden Übertragungsweg voreinstellen
<automatisch ermitteln>

Kontospezifische Skripte für den Export
Ausgänge: <keine> Vormerkposten: <keine>

Umsätze: <keine>

Die hier eingetragenen Skripte werden nur verwendet, wenn die globale Einstellung "Kontoumsätze exportieren" auf dem Reiter "Kontoinformationen" im Einstellungen-Dialog aktiviert ist.

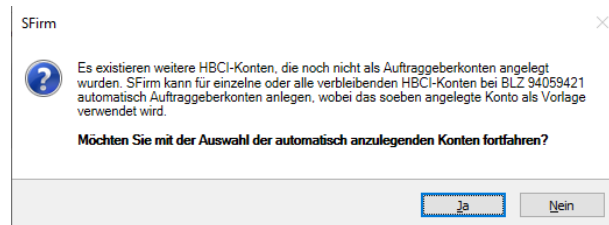
SEPA-Dateien erstellen nach Version (DFU-Abkommen, Anlage 3)
3.1/3.2/3.3

Die Einstellung gilt für alle Konten dieses Instituts. Bitte setzen Sie sich mit Ihrem Institut in Verbindung, bevor Sie diese Einstellung verändern.

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.



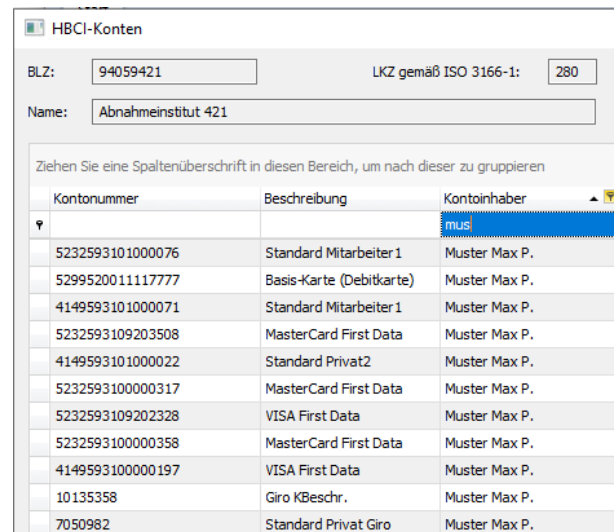
SFirm

Es existieren weitere HBCI-Konten, die noch nicht als Auftraggeberkonten angelegt wurden. SFirm kann für einzelne oder alle verbleibenden HBCI-Konten bei BLZ 94059421 automatisch Auftraggeberkonten anlegen, wobei das soeben angelegte Konto als Vorlage verwendet wird.

Möchten Sie mit der Auswahl der automatisch anzulegenden Konten fortfahren?

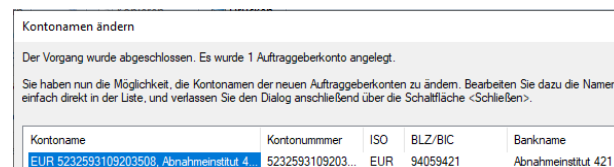
Ja Nein

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.



Kontonummer	Beschreibung	Kontoinhaber
5232593101000076	Standard Mitarbeiter1	Muster Max P.
5299520011117777	Basis-Karte (Debitkarte)	Muster Max P.
4149593101000071	Standard Mitarbeiter1	Muster Max P.
5232593109203508	MasterCard First Data	Muster Max P.
4149593101000022	Standard Privat2	Muster Max P.
5232593100000317	MasterCard First Data	Muster Max P.
5232593109202328	VISA First Data	Muster Max P.
5232593100000358	MasterCard First Data	Muster Max P.
4149593100000197	VISA First Data	Muster Max P.
10135358	Giro KBesch.	Muster Max P.
7050982	Standard Privat Giro	Muster Max P.

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

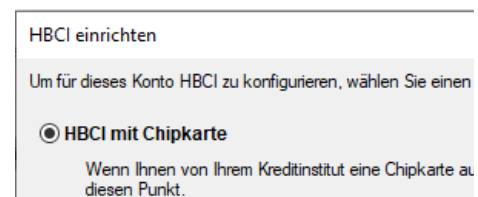


Kontoname	Kontonummer	ISO	BLZ/BIC	Bankname
EUR 5232593109203508, Abnahmeinstitut 4...	5232593109203...	EUR	94059421	Abnahmeinstitut 421

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 Auftraggeberkonto 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.

Sicherheitsmedium:	DDV-Chipkarte (Typ 1) mit Kennung SFIRM
Lokalisierung:	Kartenleser funktioniert, REINER SCT
Bank:	Abnahme-Institut 421
Interner Benutzername:	SFIRM
Benutzerkennung:	1571952702
PIN:	<input type="text"/>
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

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



Die Einrichtung des HBCI Übertragungswegs für dieses Konto ist abgeschlossen.

Nähere Informationen über Ihre Zugangsdaten und Kontoberechtigungen finden Sie auf der HBCI-Registerkarte.

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:

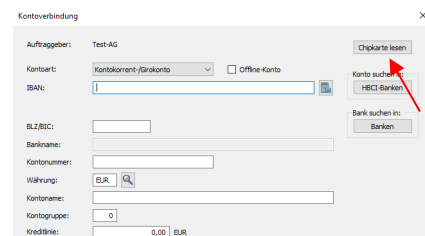
- Secoder-Produkte nach Spezifikation V2.2 im Applikationsmodus
- Klasse-3-Leser mit zwingender PIN-Eingabe über die Lesertastatur, ohne Verwendung des Displays für die Darstellung von Transaktionsdaten
- Klasse-2-Leser mit zwingender PIN-Eingabe über die Lesertastatur

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](#).

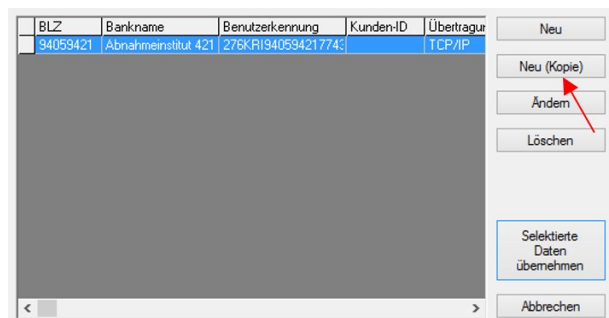
2.3.2 Neuanlage eines Kontos HBCI-Kontos mit einem RAH-7 Medium

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.

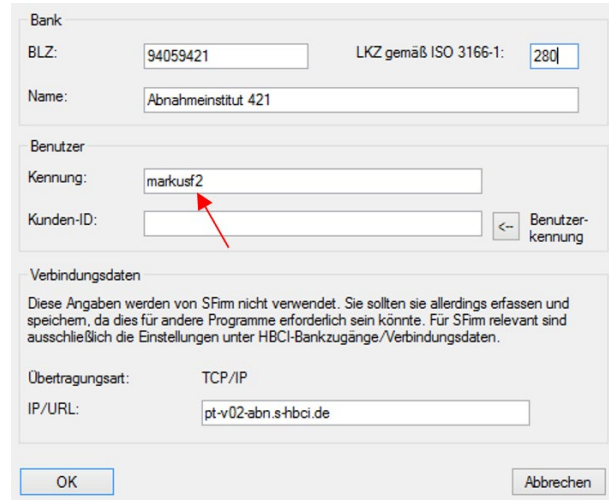
Nach der Eingabe der Karten-PIN, werden die auf der Karte befindlichen und für die Anzeige erforderlichen Daten ausgelesen und in dem Dialog *SECCOS 6 Chipkarte (rah7)* angezeigt. Auf der Chipkarte befindet sich i.d.R. bereits ein Datensatz, der durch den HBCI-Service-Client aufgebracht wurde. Erstellen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



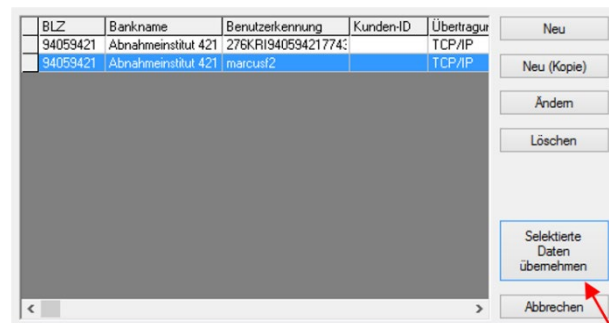


Der vom HBCI-Service-Client aufgebrachte Datensatz kann nicht übernommen werden. Der Datensatz muss durch <Neu (Kopie)> kopiert werden.

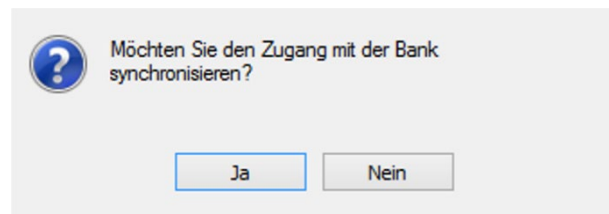
Überschreiben Sie die vorhandene Kennung mit Ihrem persönlichen Anmeldenaamen bzw. der Legitimations-ID des HBCI-Vertrags und bestätigen dies bitte mit <OK>.



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.

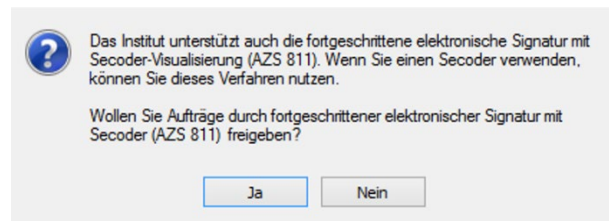


Bestätigen Sie bitte die Meldung mit <Ja>. Nach erfolgter Eingabe der PIN findet der Schlüsselaustausch mit dem Rechenzentrum, sowie das Abholen der Bank- und Benutzerdaten statt.

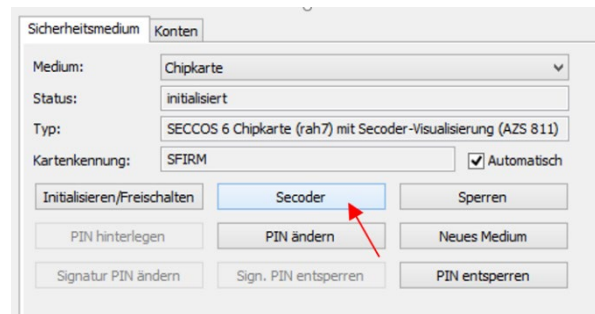




Beachten Sie bitte, dass die PIN während des Dialogs mehrfach abgefragt wird. Das resultiert aus dem Verschlüsselungskonzept des Sicherheitsmediums.

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.

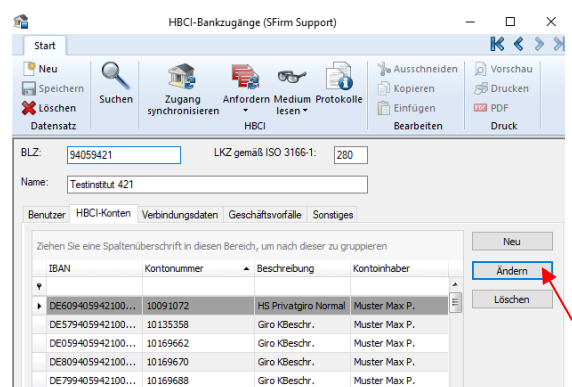
Im Folgenden wird auf die Varianten näher eingegangen, die den überwiegenden Teil der zum Einsatz kommenden RDH-Karten abdecken sollte:

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.

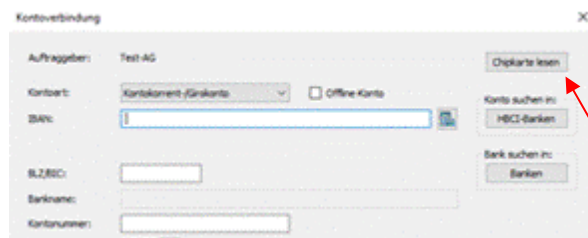
2.4.1 Kontoanlage mit einer vorbelegten RDH-Karte

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:

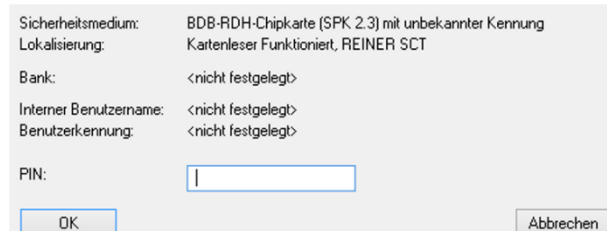
Öffnen Sie über *Stammdaten ▶ Auftraggeber* mit einem Doppelklick den Auftraggeber, dem Sie das Konto zuordnen wollen. Auf dem Reiter *Bankkonten* sehen Sie zunächst nur die bereits eingerichteten Konten. Über die Schaltfläche <Neu> gelangen Sie zu dem Dialog *Kontoverbindung*.



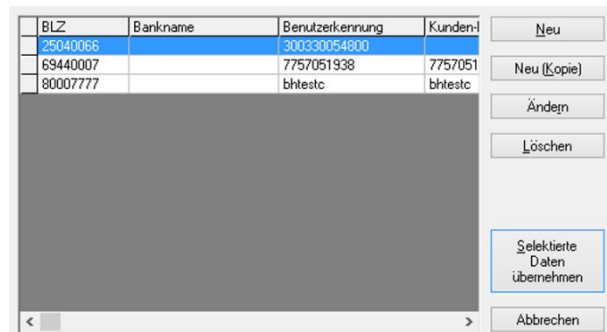
In der leeren Erfassungsmaske zur Neu-
anlage eines Kontos sehen Sie auf der
rechten Seite mehrere Schaltflächen. Kli-
cken Sie hier auf die Schaltfläche <Chip-
karte lesen>.



Zur Authentisierung des Kartenzugriffs
wird die PIN abgefragt. Nach der Eingabe
der PIN und der Bestätigung über die
Schaltfläche <OK> werden die Bankda-
ten, die auf der Karte enthalten sind, an-
gezeigt.



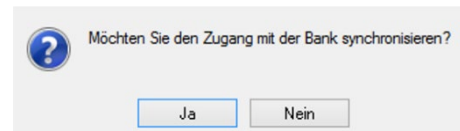
In dem Dialogtitel wird die Bezeichnung
des Sicherheitsmediums eingeblendet. In
der Regel findet sich dort nur ein Eintrag.
Wählen Sie bei mehreren den entspre-
chenden aus (durch ein Kreuz in der ers-
ten Spalte markieren) und klicken Sie auf
die Schaltfläche <Selektierte Daten über-
nehmen>.



BLZ	Bankname	Benutzerkennung	Kunden-ID
25040066		300330054800	
69440007		7757051938	7757051
80007777		bhstestc	bhstestc

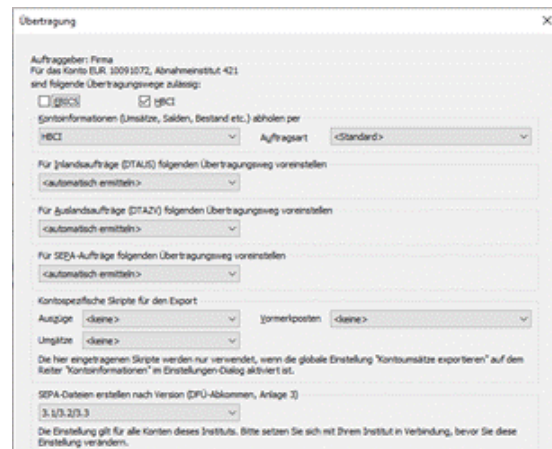
2.4.1.1 Selektierte Daten übernehmen

Anschließend können Sie den Zugang synchronisie-
ren. Bestätigen Sie hierzu den nebenstehenden Dia-
log 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 Be-
stätigung der Schaltfläche <OK>, erscheint
der Dialog *Übertragung*. Der Übertragungs-
weg *HBCI* wird nun automatisch markiert an-
gezeigt. Ebenso auch die Abholung der Kon-
toumsätze per HBCI. Automatisch ermittelt
wird der Übertragungsweg für den Transfer
von DTAUS und DTAZV und SEPA-
Aufträgen.



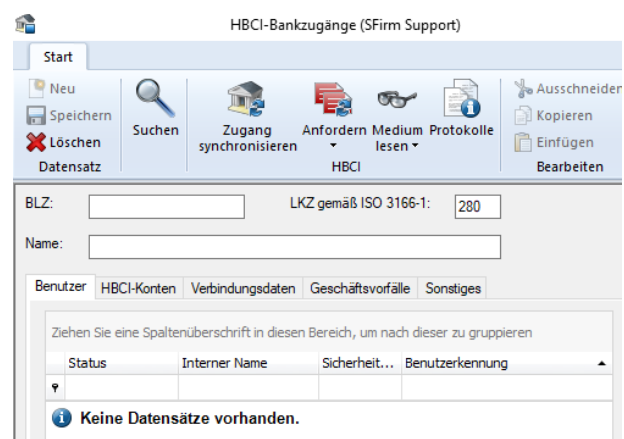
Mit den <Weiter>-Schaltflächen werden weitere Dialoge angezeigt. Zu diesen gehören je nach lizenzierten Modulen die Dialoge *Cash*, *Depooling*, *AZV*, *MT101*, *HBCI*, und *Rundrufdefinition*. Nach Bestätigung der Schaltfläche <Fertig stellen> ist die Kontoanlage abgeschlossen. Sollten mit der Synchronisation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

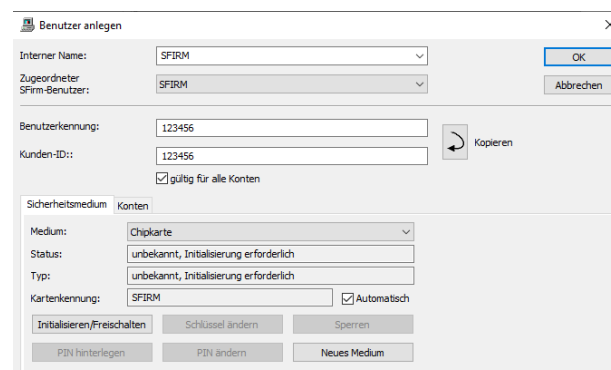
In diesem Abschnitt wird eine Kontoanlage mit einer leeren RDH-Karte beschrieben, die keine Bankdaten, keine Benutzererkennung und keine Schlüssel enthält. Die Karten-PIN wurde ebenfalls noch nicht hinterlegt. Zur besseren Übersicht wird die Einrichtung hier über *Stammdaten* ▶ *Bankzugänge* ▶ *HBCI* ▶ *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 Benutzererkennung und Verbindungsdaten werden Ihnen vom Kundenberater mitgeteilt und hier erfasst. Die Angaben der Benutzererkennung 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>.

Initialisieren/Freischalten ×

Sicherheitsmedium:	Chipkarte mit Kennung SFIRM
Spezifikation:	Chipkarte mit Kennung SFIRM
Lokalisierung:	Kartenleser REINER SCT cyberJack Secoder USB 1, REINER
Bank:	Testinstitut 421
Interner Benutzername:	SFIRM
Benutzerkennung:	321321

Bitte legen Sie die Chipkarte in den Kartenleser.

Weiter Abbrechen

2.4.2.2 Die PIN hinterlegen

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

Sicherheitsmedium:	Chipkarte mit unbekannter Kennung
Lokalisierung:	Kartenleser cyberJack USB, REINER SCT
Bank:	<nicht festgelegt>
Interner Benutzername:	<nicht festgelegt>
Benutzerkennung:	<nicht festgelegt>

Ihre Chipkarte verfügt noch nicht über eine PIN. Bitte geben Sie jetzt eine von Ihnen frei wählbare PIN ein, mit der die Karte geschützt wird.

PIN:

Wiederholung:

Bitte merken Sie sich Ihre Eingabe.
Sie werden bei jedem Zugriff auf das Medium danach gefragt.

OK Abbrechen

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>.

Sicherheitsmedium:	BDB-RDH-Chipkarte (SPK 2.3) mit Kennung SFIRM
Spezifikation:	BDB-RDH-Chipkarte (SPK 2.3) mit Kennung SFIRM
Lokalisierung:	Kartenleser cyberJack USB, REINER SCT
Bank:	Testinstitut
Interner Benutzername:	SFIRM
Benutzerkennung:	bhtestc

Es liegt eine BDB-RDH-Chipkarte (SPK 2.3) vor.
Die Chipkarte enthält bereits Daten und wird zusätzlich für obigen Benutzer initialisiert.

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>.

Sicherheitsmedium:	BDB-RDH-Chipkarte (SPK 2.3) mit Kennung SFIRM
Spezifikation:	BDB-RDH-Chipkarte (SPK 2.3) mit Kennung SFIRM
Lokalisierung:	Kartenleser cyberJack USB, REINER SCT
Bank:	Testinstitut
Interner Benutzername:	SFIRM
Benutzerkennung:	bhtestc

Die Benutzerdaten und Benutzerschlüssel sind jetzt angelegt.
Drücken Sie auf <Weiter>, um Ihre Schlüssel mit der Bank auszutauschen.

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

Es wird das folgende Sicherheitsmedium benötigt:

Spezifikation:	BDB-RDH-Chipkarte (SPK 2.3) mit Kennung SFIRM
Lokalisierung:	Kartenleser cybeslack USB, REINER SCT
Bank:	Testinstitut
Interner Benutzername:	SFIRM
Benutzerkennung:	bh1estc

Bitte legen Sie das Sicherheitsmedium ein, und klicken Sie auf auf <OK>.

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.

Bank: Testinstitut

Der Hashwert des öffentlichen Signierschlüssels der Bank lautet:

8E	56	9B	B6	AA	00	4A	F8	29	AD
D2	D4	D1	9B	79	7D	8C	5C	19	64

Vergleichen Sie diesen Wert mit dem Wert, den Ihnen Ihre Bank mitgeteilt hat. Nur bei Übereinstimmung ist die Authentizität gewährleistet. Stimmen die Werte überein?

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 Schlüssels darstellt. Drucken Sie den Brief über die Schaltfläche <INI-Brief drucken> aus. Dieser Brief ist unterschrieben an das Institut weiterzuleiten.

Sicherheitsmedium

Spezifikation:	BDB-RDH-Chipkarte (SPK 2.3) mit Kennung SFIRM
Lokalisierung:	Kartenleser cybeslack USB, REINER SCT
Bank:	Testinstitut
Interner Benutzername:	SFIRM
Benutzerkennung:	bh1estc

Das Medium ist für den Benutzer initialisiert. Der Hashwert des öffentlichen Benutzer-Signierschlüssels lautet:

4E	2E	91	13	4D	DF	C8	50	90	8E
A7	5F	5D	F0	58	B1	E7	62	90	5F

☒ Formatierte Anzeige

Nach SFirm32 vorliegenden Informationen ist eine Bestätigung des Benutzerschlüssels bei der Bank erforderlich. Dies kann durch einen INI-Brief geschehen, den Sie hier drucken können.

Anzahl:

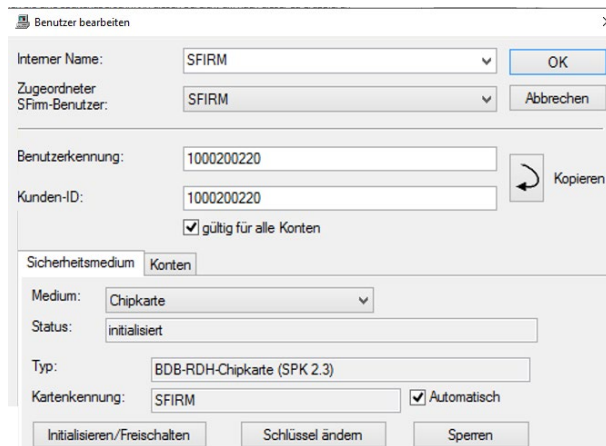
Die Freischaltung der Benutzerschlüssel kann auf Institutsseite mehrere Tage in Anspruch nehmen.



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.



Kontonummer	Kontoart
2512162523	Tagesgeld
2512162533	Geschäft
2512162543	Spenden
2512162553	Festgeld

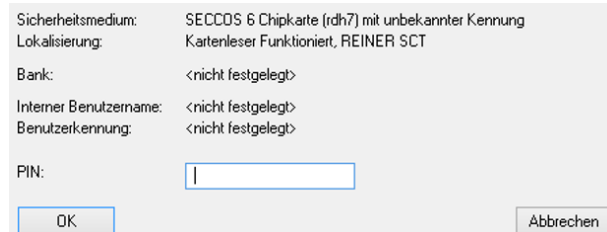
Mit den <Weiter>-Schaltflächen werden weitere Dialoge angezeigt. Zu diesen gehören je nach lizenzierten Modulen die Dialoge *Cash*, *Depooling*, *AZV*, *MT101*, *HBCI*, und *Rundrufdefinition*. Nach Bestätigung der Schaltfläche <Fertig stellen> ist die Kontoanlage abgeschlossen. Sollten mit der Synchronisation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

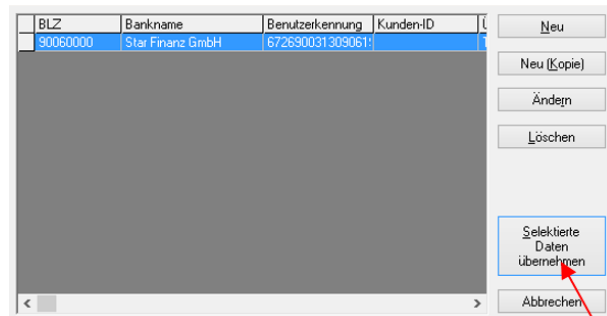
Sie erhalten die Karte und eine dazu gehörige 6-stellige PIN. Sie haben die Möglichkeit diese PIN zu ändern, dies ist jedoch nicht erforderlich.

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



Sicherheitsmedium: SECCOS 6 Chipkarte (rdh7) mit unbekannter Kennung
Lokalisierung: Kartenleser funktioniert, REINER SCT
Bank: <nicht festgelegt>
Interner Benutzername: <nicht festgelegt>
Benutzerkennung: <nicht festgelegt>
PIN:
OK Abbrechen

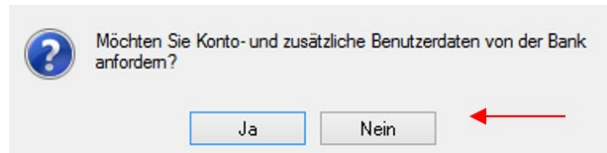
Im nächsten Schritt erscheint die Auflistung der auf der HBCI-Karte vorhandenen Datensätze. Markieren Sie den gewünschten Datensatz und klicken bitte auf <Selektierte Daten übernehmen>



BLZ	Bankname	Benutzerkennung	Kunden-ID
90060000	Star Finanz GmbH	672690031309061	

Neu
Neu (Kopie)
Ändern
Löschen
Selektierte Daten übernehmen
Abbrechen

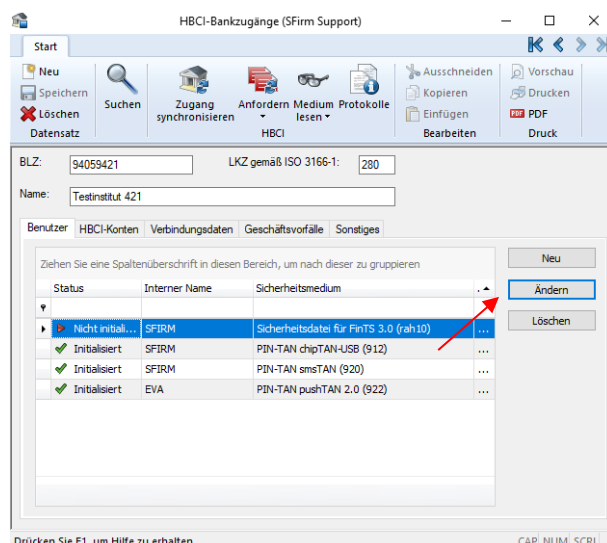
Die Frage im nebenstehenden Dialog beantworten Sie bitte mit <Nein>



Möchten Sie Konto- und zusätzliche Benutzerdaten von der Bank anfordern?
Ja Nein

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

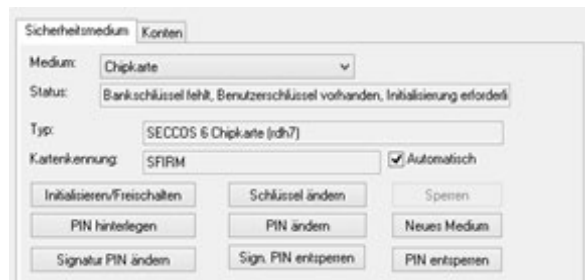
Klicken Sie bitte auf <Ändern> um in den Dialog <Benutzer bearbeiten> zu gelangen.



HBCI-Bankzugänge (SFirm Support)
Start
Neu Suchen Zugang synchronisieren Anfordern Medium Protokolle lesen HBCI Ausschneiden Kopieren Einfügen Bearbeiten Vorschau Drucken PDF Druck
BLZ: 94059421 LKZ gemäß ISO 3166-1: 280
Name: Testinstitut 421
Benutzer HBCI-Konten Verbindungsdaten Geschäftsvorfälle Sonstiges
Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser zu gruppieren
Status Interner Name Sicherheitsmedium
Nicht initialisiert SFIRM Sicherheitsdatei für FinTS 3.0 (rah10)
Initialisiert SFIRM PIN-TAN chipTAN-USB (912)
Initialisiert SFIRM PIN-TAN smsTAN (920)
Initialisiert EVA PIN-TAN pushTAN 2.0 (922)
Neu Ändern Löschen
Drücken Sie F1, um Hilfe zu erhalten. CAP: NUM: SCRL: ..

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

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 Kartensperkung 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>.



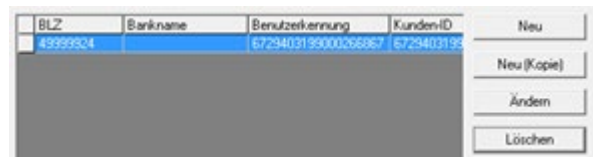
Im folgenden Dialog ist nun eine vom Benutzer selbst kreierte numerische Karten-PIN einzugeben, die in Zukunft für den Kartenzugriff Verwendung finden soll. Die PIN-Länge muss aus 6 bis 8 Zahlen bestehen. Aufgrund der verdeckten Eingabe muss diese wiederholt werden. Bestätigen Sie anschließend die Eingaben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

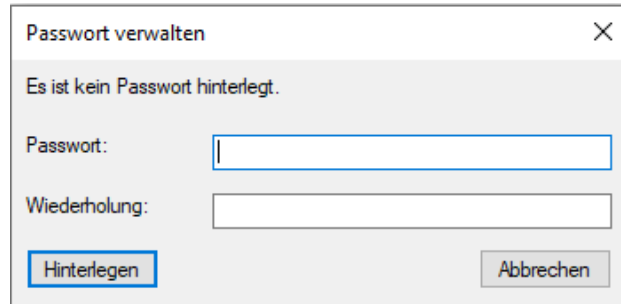


BLZ	Bankname	Benutzerkennung	KundenID
49999924		672940319900006687	6729403199

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>.

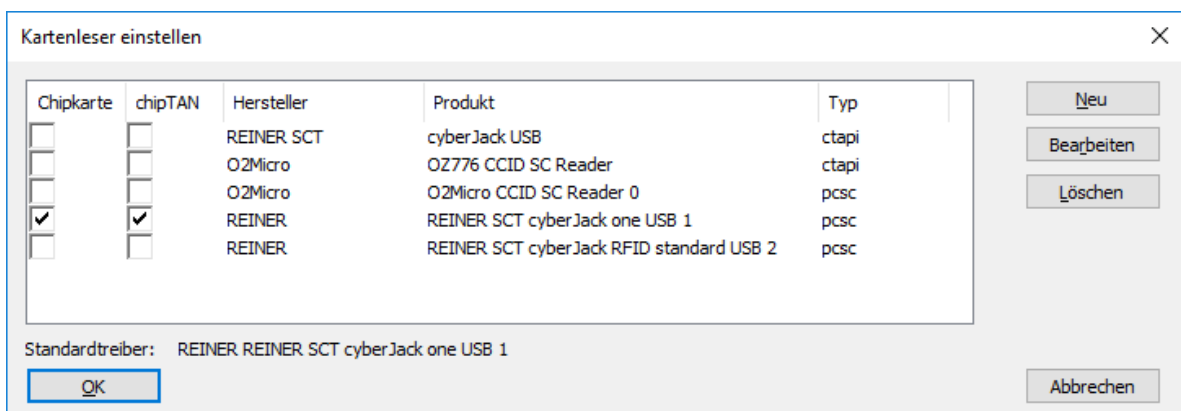


Sofern Sie keinen Klasse-2-Kartenleser verwenden und ein PIN hinterlegt haben, entfallen bei Zugriffen auf die Chipkarte die Aufforderungen zur PIN-Eingabe. Bitte beachten Sie, dass durch das Hinterlegen einer PIN das Risiko einer unbefugten Benutzung des Sicherheitsmediums besteht.

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.




Chipkarte	chipTAN	Hersteller	Produkt	Typ
<input type="checkbox"/>	<input type="checkbox"/>	REINER SCT	cyberJack USB	ctapi
<input type="checkbox"/>	<input type="checkbox"/>	O2Micro	OZ776 CCID SC Reader	ctapi
<input type="checkbox"/>	<input type="checkbox"/>	O2Micro	OZ776 CCID SC Reader 0	pcsc
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	REINER	REINER SCT cyberJack one USB 1	pcsc
<input type="checkbox"/>	<input type="checkbox"/>	REINER	REINER SCT cyberJack RFID standard USB 2	pcsc

Standardtreiber: REINER REINER SCT cyberJack one USB 1

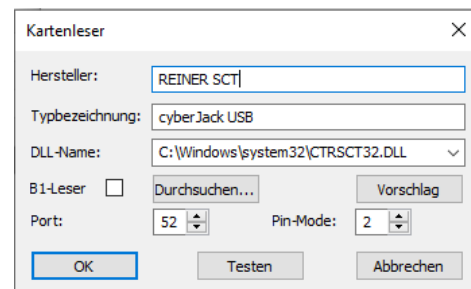
Sie sehen die in SFirm eingerichteten Kartenleser. Einige Kartenleser unterstützen sowohl das HBCI-Chipkartenverfahren (DDV, RAH, RDH), wie auch die chipTAN USB Funktionali-

tät. 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:

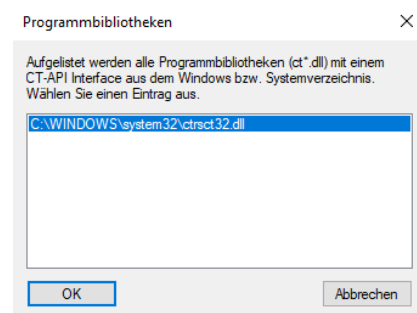


Hersteller	Geben Sie hier einen individuellen Text für den Hersteller ein. Der Inhalt dieses Feldes hat einen rein informativen Charakter und kann beliebig gefüllt werden.
Typ	Geben Sie hier einen individuellen Text für den Typ des Kartenlesers ein. Der Inhalt dieses Feldes hat einen rein informativen Charakter und kann beliebig gefüllt werden.
DLL-Name	Im Feld <i>DLL-Name</i> 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 <i>Programmbibliotheken</i> .
<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.

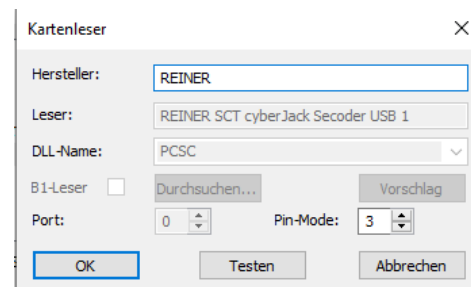


Diese Treiber-DLL ist von Ihnen auszuwählen. Im Zweifel wenden Sie sich bitte an den Hersteller Ihres Kartenlesers.

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.

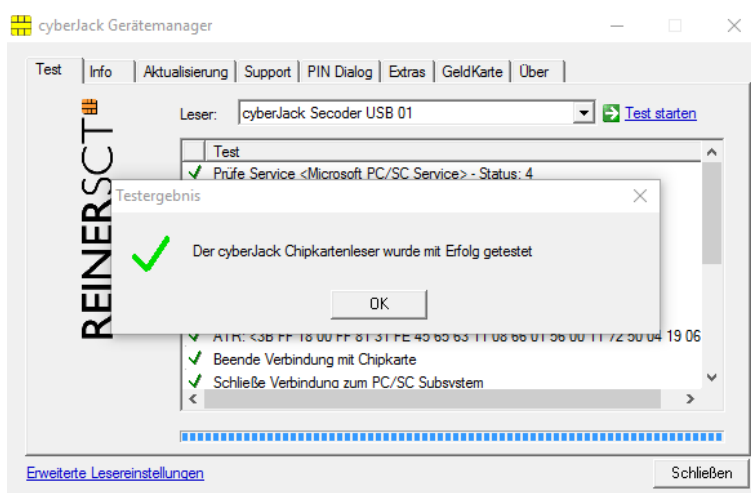


Die Einrichtung und Konfiguration üblicher Kartenlesegeräte sollte durch einen fachkundigen Systemadministrator durchgeführt werden. Da sich die Einrichtung, in unserer Testumgebung, teilweise als sehr schwierig gestaltet hat und dessen Erfolg von vielen Systemumgebungsfaktoren abhängt, können wir hierzu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

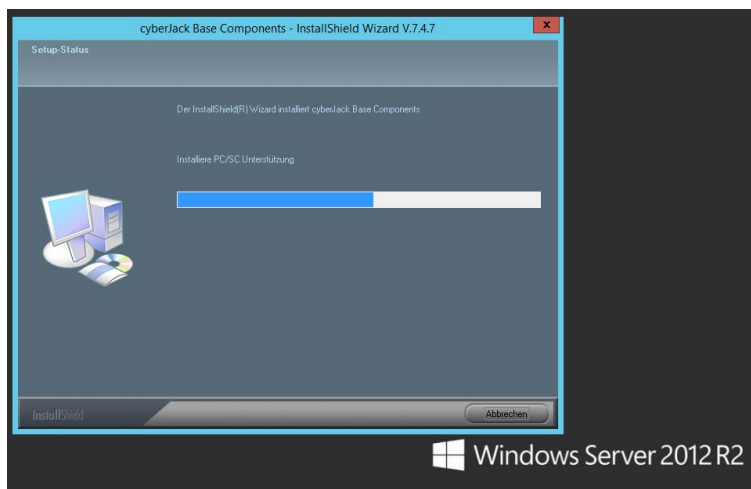
2.6.2.2 Einrichtung

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.

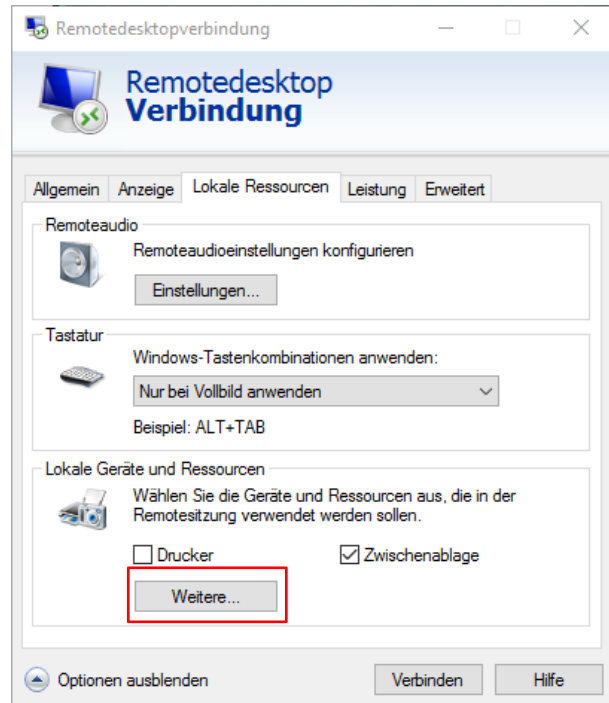


- i** Genaue Spezifikationen und eventuelle Einschränkungen der Funktionalitäten sind den Internetseiten des Kartenleser-Herstellers oder über deren Kundenservice zu erfragen.

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

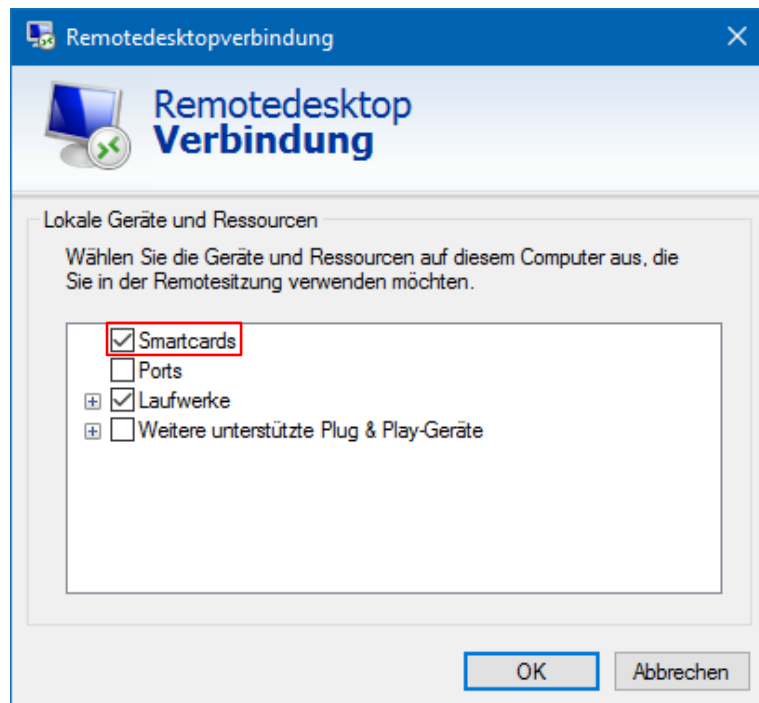
Dies ist in der Einrichtung vergleichbar mit lokalen Laufwerken. Im Regelfall ist diese Einstellung bereits aktiv.

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.



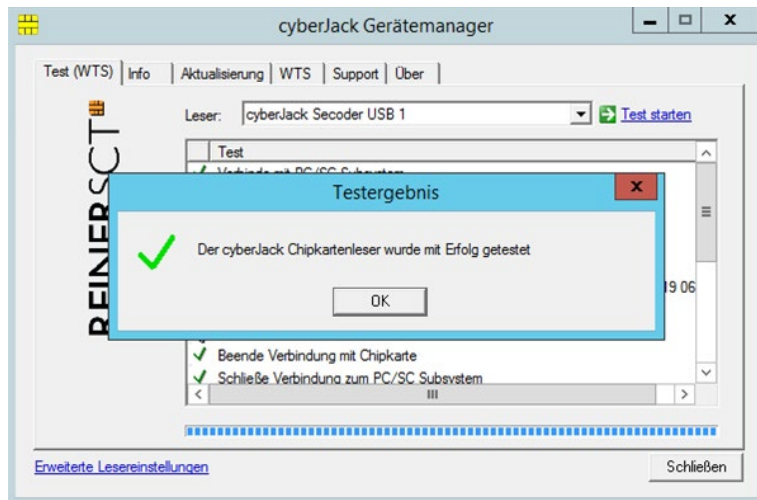
Im Regelfall ist diese Einstellung bereits aktiv. Diese Einstellung kann der Anwender in der Remotedesktopverbindung durchführen oder die Systemadministratoren haben die Möglichkeit, dieses für den Anwender vorzugeben.

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

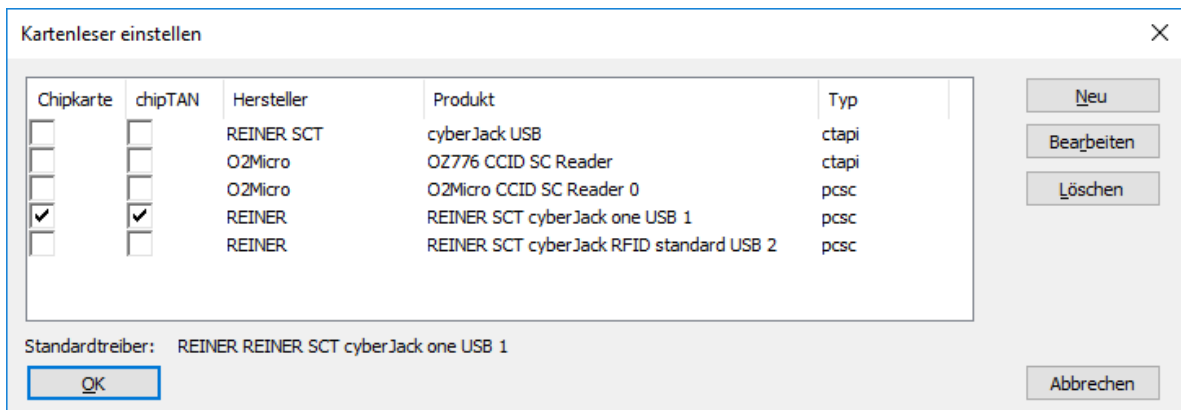


- i** In SFirm ist direkt nach der Installation des Kartenlesertreibers ein neuer Kartenleser des Typs CT-API verfügbar. Erst wenn die o.g. Smartcard-Einstellung aktiv ist, wird ein weiterer Kartenleser des Typs PC/SC sichtbar.

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. Verlieft 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

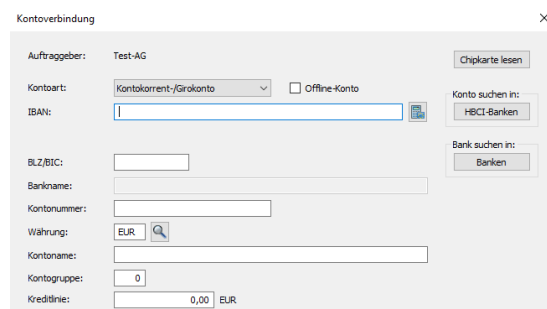
Konfiguration der Übertragungswege

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

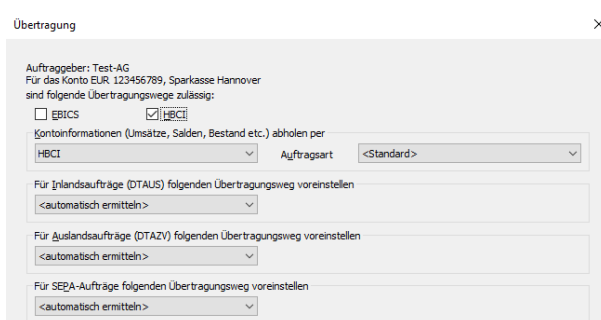
3.2 Erfassung einer Kontoverbindung

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.

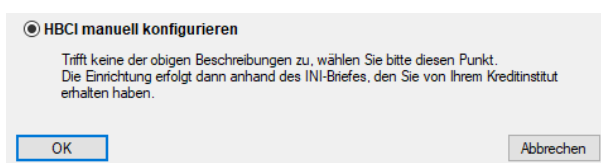


Als Übertragungsweg ist das Verfahren *HBCI* auszuwählen. Das Abholen der Kontoumsätze mit HBCI wird automatisch vorbelegt. Klicken Sie auf <Weiter> und definieren Sie die Parameter für die weiteren Module von SFirm.

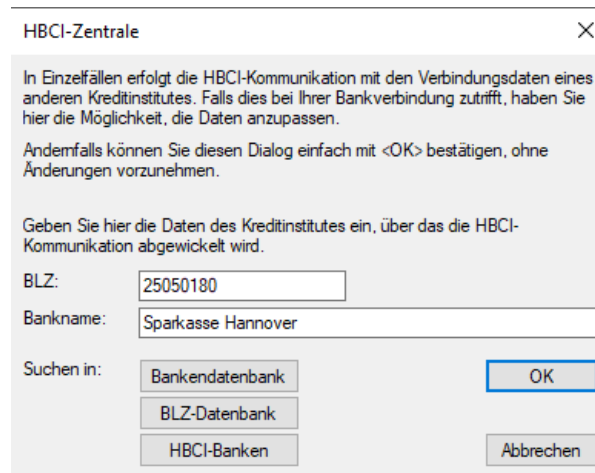


3.3 Der Assistent zur manuellen Konfiguration

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>.

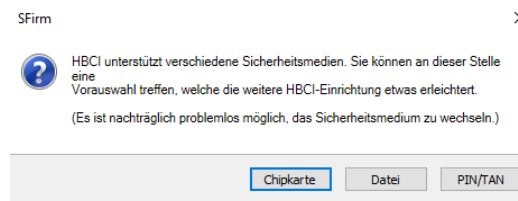


I.d.R. werden die Angaben des vorbelegten Instituts übernommen und können mit <OK> bestätigt werden.



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>.

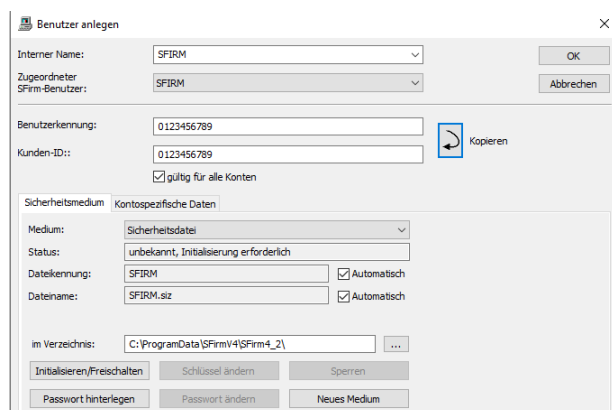
Bestätigen Sie im nächsten Dialog als Sicherheitsmedium <Datei>, damit die Schlüssel auf einer Sicherheitsdatei gespeichert werden.



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

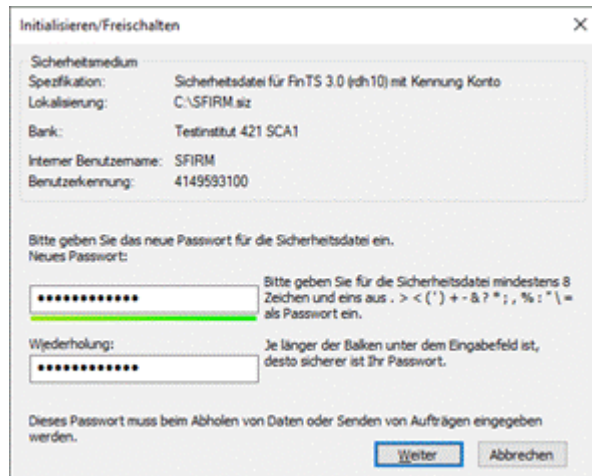
Geben Sie die vom Institut mitgeteilte Benutzerkennung ein. Häufig stimmt die Kunden-ID mit der Benutzerkennung überein. Vergibt die Bank keine Kunden-ID, ist in diesem Fall das Feld mit der Benutzerkennung zu erfassen. Als Medium ist bereits *Sicherheitsdatei* ausgewählt. Das Kontrollfeld *gültig für 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 Wechsel-datenträger 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 Benutzer-schlüssel 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.

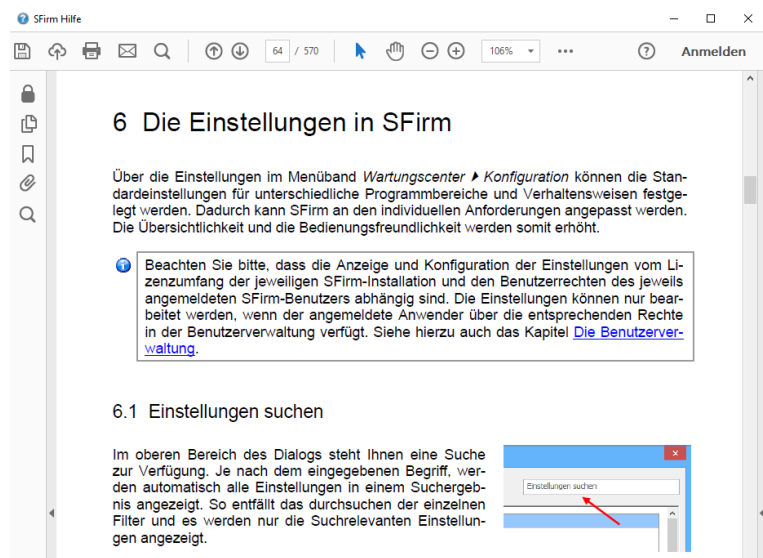
4 Weitere Informationsquellen & Support

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.

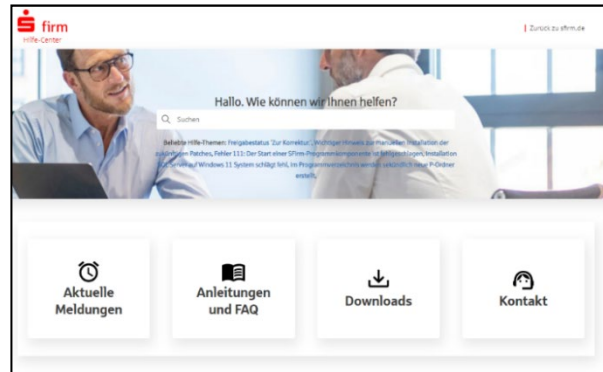


4.2 Der Internetauftritt von SFirm

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 Hilfe-Center

Das SFirm Hilfe-Center enthält eine Wissensdatenbank, die Informationen, Hinweise und Problemlösungen zu den aktuellen, freigegebenen Versionen von SFirm strukturiert zur Verfügung stellt. Alle Informationen finden Sie auf hilfe.sfirm.de.



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 die Seite seminare.starfinanz.de. 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 / 71 55 99 0 (2,49 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 Grüner Deich 15 20097 Hamburg
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 / 71 55 99 0 (2,49 EUR/Minute inkl. MwSt. aus dem deutschen Festnetz; abweichende Preise für Mobilfunkteilnehmer).