firm

Kundenleitfaden
Umstellung der EBICS-EU

Finanzen. Professionell. Managen.

Dezember 2024

Inhalt

1 Umstellung der elektronischen Unterschrift....3

1.1 Allgemein....3
1.1.1 Umstellung im laufenden Betrieb....3
1.1.2 Schlüsseländerungen und Ersatz von Schlüsseln....4
1.2 EU-Schlüsseländerung....4
1.2.1 EU-Schlüsseländerung mit Sicherheitsdatei....4
1.2.2 EU-Schlüsseländerung mit Signaturkarte....6
1.3 Benutzerinitialisierung über die EBICS-Schlüsselverwaltung....7
1.3.1 Ersetzen von EU-Schlüsseln....8
1.4 Änderung des Authentifikationsschlüssels....9
1.4.1 Ersetzen des Authentifikationsschlüssels....10
1.5 Bankschlüssel abholen....11

2 Weitere Informationsquellen & Support....13

2.1 Die Hilfe in SFirm....13
2.2 Der Internetauftritt von SFirm....13
2.2.1 SFirm Hilfe-Center....14
2.2.2 Seminare....14
2.3 Der technische Kundenservice....14
2.4 Kontaktinformationen....15

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 Umstellung der elektronischen Unterschrift

1.1 Allgemein

In SFirm ist die Verwendung von bestehenden A004-EU-Schlüsseln möglich, bei einer Neuerzeugung werden standardmäßig A006-EU-Schlüssel für die elektronische Unterschrift erzeugt. Beide können erzeugt oder von SECCOS-Chipkarten gelesen und genutzt werden. Eine Änderung des EU-Schlüssels ist optional, kann aber aufgrund einer neuen EBICS-Version obligatorisch ausfallen. Auch wenn Ihre bisherigen bestehenden A004-EU-Schlüssel weiterhin genutzt werden können, empfehlen wir aus Sicherheitsgründen jedoch immer die Umstellung auf die aktuelle Version.

1.1.1 Umstellung im laufenden Betrieb

Wenn im laufenden Betrieb eine neue EU erzeugt wird (z.B. vorher A004/A005, neu A006), kann diese in der EBICS-Schlüsselverwaltung über die Schaltfläche <Schlüssel senden> als EU-Schlüsseländerung an alle beteiligten Kreditinstitute gesendet werden, eine Neuinitialisierung ist nicht nötig. Der Ablauf:

- Rufen Sie die EBICS-Schlüsselverwaltung innerhalb der *Stammdaten ▸ Bankzugänge ▸ EBICS* über das Menüband *Start ▸ EBICS ▸ EBICS-Schlüsselverwaltung* auf.
- Markieren Sie bitte den ersten Eintrag des Kreditinstituts, an das der neue Schlüssel gesendet werden soll.
- Klicken Sie auf die Schaltfläche <Schlüssel senden> und folgen dem Dialog.
- In der Spalte *Status* können Sie anhand des Eintrags PUB (für EU-Schlüsseländerung) erkennen, an welche Institute die Schlüssel noch gesendet werden müssen. Sobald ein Eintrag des Status *bereit* hat, war das Senden der Schlüsseländerung erfolgreich.
- Markieren Sie den nächsten Eintrag, bei dem in der Spalte *Status* der Eintrag PUB steht. Klicken Sie erneut auf die Schaltfläche <Schlüssel senden> und folgen dem Dialog.

Wiederholen Sie die letzten beiden Schritte für alle Einträge in der EBICS-Schlüsselverwaltung, d.h. für alle Kreditinstitute, bis alle in der Spalte *Status* den Eintrag *bereit* haben.

Unter Umständen erscheint in SFirm auf der Startseite eine Aufgabe, die über eine bevorstehende obligatorische Schlüsseländerung informiert und den angemeldeten Benutzer durch die Umstellung leitet.

1.1.2 Schlüsseländerungen und Ersatz von Schlüsseln

Aus unterschiedlichen Gründen kann es notwendig werden, den EU-Schlüssel oder Authentifizierungsschlüssel eines Teilnehmers zu ändern oder zu erneuern. In den folgenden Abschnitten werden vier mögliche Eingriffe beschrieben.

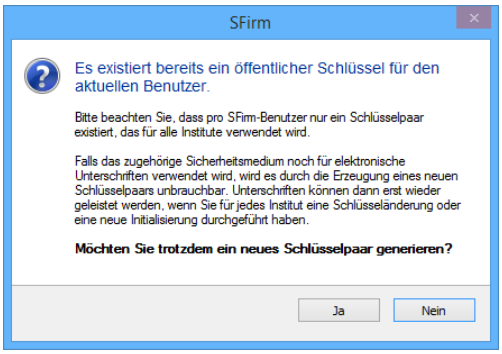
> Stellen Sie in jedem Fall sicher, dass eine Anmeldung als *der* Benutzer vorliegt, für den die Änderung vorgenommen werden soll. Weiterhin wird in den folgenden Beschreibungen davon ausgegangen, dass ein Bankschlüssel zu dem Host bereits vorhanden ist (siehe Abschnitt Bankschlüssel abholen).

1.2 EU-Schlüsseländerung

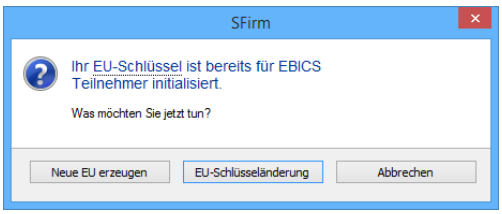
In diesem Abschnitt wird davon ausgegangen, dass ein EU-Schlüsselpaar vorhanden ist, das dazugehörige Kennwort bekannt ist und eine Schlüsseländerung vorgenommen werden soll.

1.2.1 EU-Schlüsseländerung mit Sicherheitsdatei

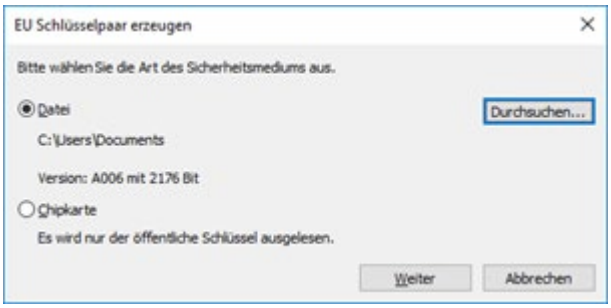
Rufen Sie die Funktion *EU Schlüssel erzeugen* in der EBICS-Schlüsselverwaltung (*Stammdaten ▸ Bankzugänge ▸ EBICS ▸ EBICS-Schlüsselverwaltung)* auf. Sie werden auf die Tatsache aufmerksam gemacht, dass bereits ein EU-Schlüsselpaar vorhanden ist und mit einer Änderung weitere Schritte folgen müssen. Beantworten sie die Abfrage mit <Ja>.



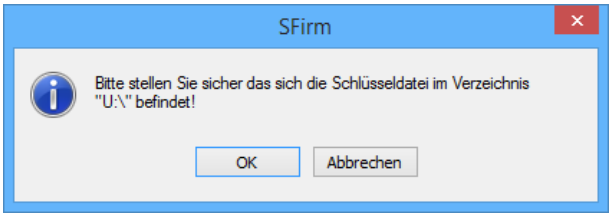
Da bereits ein initialisierter EU-Schlüssel für den angemeldeten Teilnehmer existiert, werden Sie gefragt, ob Sie einen neuen Schlüssel erzeugen oder eine Schlüsseländerung durchführen möchten. Wählen Sie hier die <EU-Schlüsseländerung>.



Wählen Sie nun das entsprechende Sicherheitsmedium aus, auf dem Sie den zukünftigen, neuen EU-Schlüssel (Private Key) ablegen möchten. Es muss sich hierbei nicht um das gleiche Sicherheitsmedium handeln, dass Sie ursprünglich für den „alten“ Schlüssel verwendet haben.



Sie werden jetzt darauf hingewiesen zu prüfen, ob sich das bisherige Sicherheitsmedium in dem gewählten Pfad befindet. In diesem Beispiel wurde das Sicherheitsmedium *Datei* verwendet.



Es folgt die Eingabe des alten EU-Kennwortes, das bei einer Schlüsseländerung vorliegen muss.

Ist dies (doch) nicht der Fall, muss das weitere Vorgehen hier abgebrochen und die Arbeitsschritte des Abschnitts Ersetzen von EU-Schlüsseln angewendet werden.

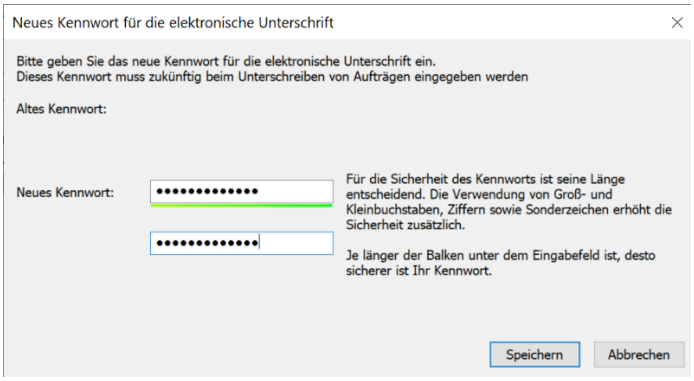
Wurde als „altes“ Medium bislang eine Chipkarte verwendet, ist nun das EU-Passwort (oder auch EU-PIN) einzugeben.

Legen Sie das neue Sicherheitsmedium in das angegebene Laufwerk ein. Bei einer ständig verfügbaren Anbindung (wie ein lokales Laufwerk) ist nichts weiter zu tun.

Nach der Bestätigung mit <OK> wird eine neue EU-Schlüsseldatei für den angemeldeten Benutzer erzeugt und in dem voreingestellten Pfad für die Schlüsseldatei gespeichert.

Existiert auf dem neuen Medium bereits eine Schlüsseldatei, werden Sie jetzt gefragt, ob diese überschrieben werden soll. Wenn es sich hier nicht um ein Versehen handelt, Antworten Sie mit <Ja>.

Geben Sie nun das neue EU-Kennwort für die elektronische Unterschrift nebst Wiederholung ein. Bestätigen Sie die Eingaben mit <Speichern>.

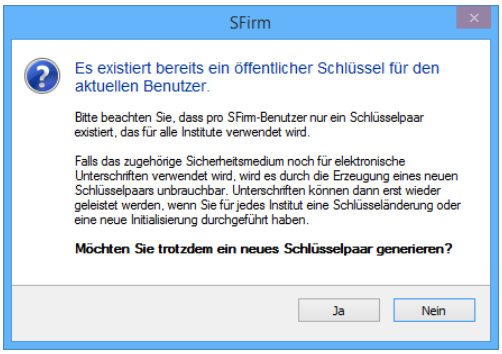


Es erscheint abschließend eine Erfolgsmeldung zur Erstellung des Schlüsselpaares. In den folgenden Unterkapiteln werden beide Wege beschrieben:

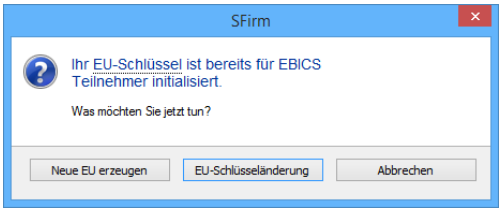
1.2.2 EU-Schlüsseländerung mit Signaturkarte

Um Ihre neue Signaturkarte zu verwenden ist es zunächst notwendig die Transport-PIN zu ändern.

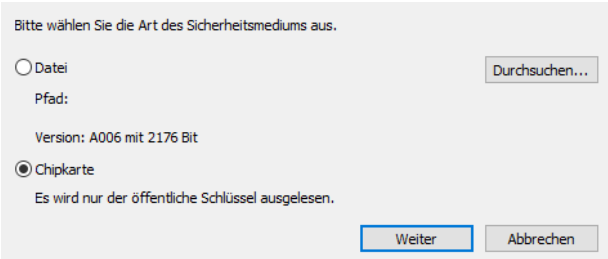
Rufen Sie die Funktion *EU Schlüssel erzeugen* in der EBICS-Schlüsselverwaltung (*Stammdaten ▸ Bankzugänge ▸ EBICS ▸ EBICS-Schlüsselverwaltung)* auf. Sie werden auf die Tatsache aufmerksam gemacht, dass bereits ein EU-Schlüsselpaar vorhanden ist und mit einer Änderung weitere Schritte folgen müssen. Beantworten sie die Abfrage mit <Ja>.



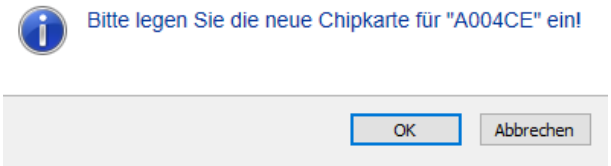
Da bereits ein initialisierter EU-Schlüssel für den angemeldeten Teilnehmer existiert, werden Sie gefragt, ob Sie einen neuen Schlüssel erzeugen oder eine Schlüsseländerung durchführen möchten. Wählen Sie hier die <EU-Schlüsseländerung>.



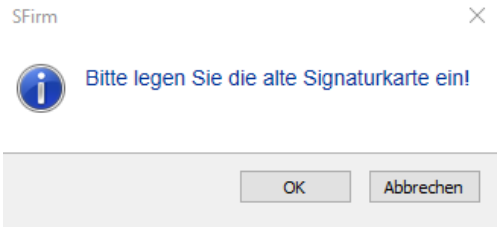
Wählen Sie nun das entsprechende Sicherheitsmedium aus, auf dem Sie den zukünftigen, neuen EU-Schlüssel (Private Key) ablegen möchten. Es muss sich hierbei nicht um das gleiche Sicherheitsmedium handeln, dass Sie ursprünglich für den „alten“ Schlüssel verwendet haben.



Sie werden aufgefordert die neue Chipkarte einzulegen.

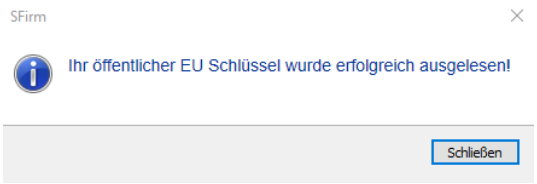


Legen Sie die alte Signaturkarte in das Kartenlesegerät ein.

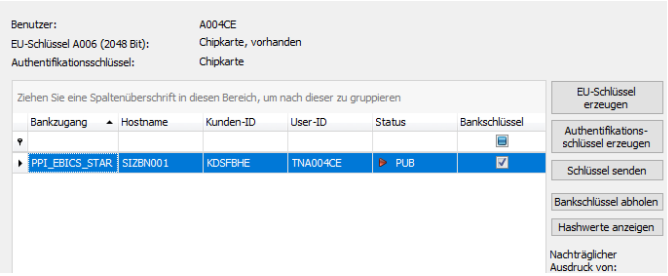


Hier müssen Sie nun die PIN der alten Signaturkarte eingeben.

Die Schlüssel wurden nun ausgelesen.

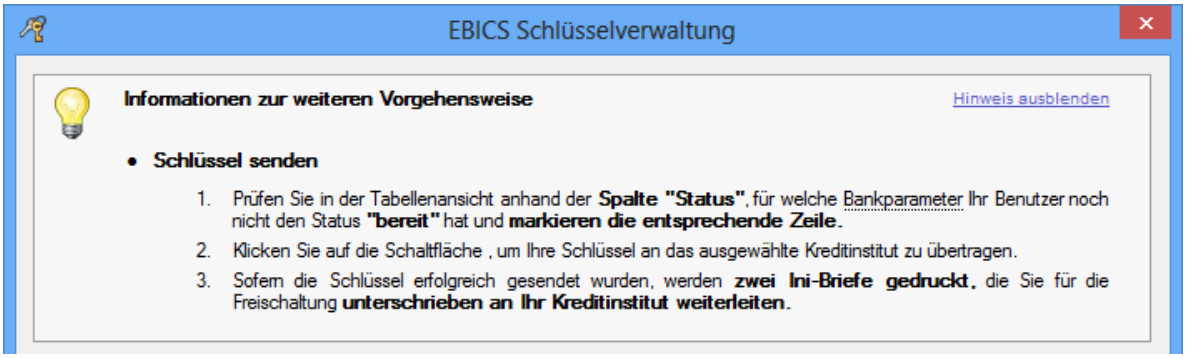


Senden Sie die Schlüssel nun an alle Institute die diese Schlüssel verwenden sollen.

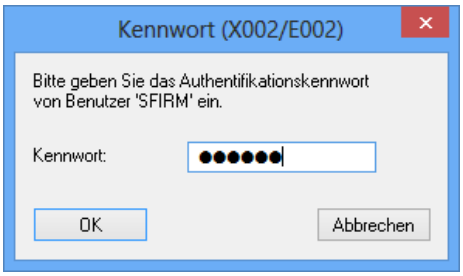


1.3 Benutzerinitialisierung über die EBICS-Schlüsselverwaltung

Wurde die EBICS-Schlüsselverwaltung über den oben angegebenen Link oder über die Hauptgruppe *Stammdaten ▸ Bankzugänge ▸ EBICS, Menüband Start ▸ EBICS ▸ EBICS-Schlüsselverwaltung* aufgerufen, sollten Sie nun folgende Information zur weiteren Vorgehensweise angezeigt bekommen:

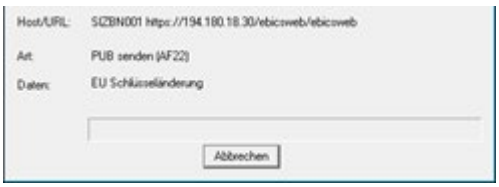


Klicken Sie nun auf die Schaltfläche <Schlüssel senden>. Da es sich hier nur um eine Schlüsseländerung des EU-Schlüssels handelt, kann der bereits initialisierte Authentifikationsschlüssel zur Autorisierung verwendet werden.



Damit entfällt die Erzeugung und Freischaltung eines Initialisierungsbriefs und der Kunde ist nach dem Senden des Schlüssels wieder arbeitsfähig.

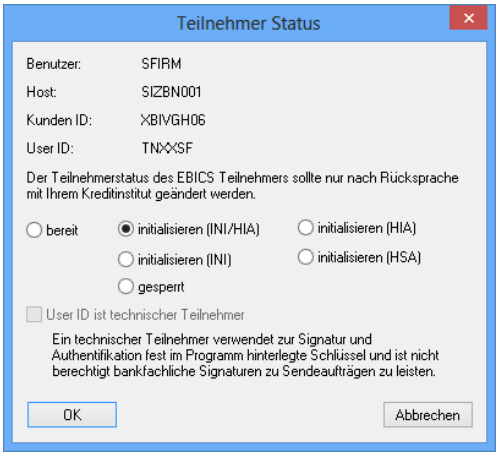
Für die EU Schlüsseländerung wird nun ein EBICS-Transfer mit der Art *PUB senden* durchgeführt. Der Transfer wird mit einer Erfolgsmeldung abgeschlossen.



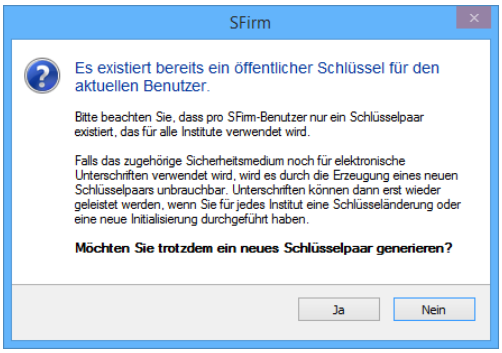
1.3.1 Ersetzen von EU-Schlüsseln

Ist die bisherige elektronische Unterschrift nicht mehr verwendbar und / oder das Kennwort nicht mehr bekannt, muss der Teilnehmer zunächst auf Seiten des Rechenzentrums zurückgesetzt werden.

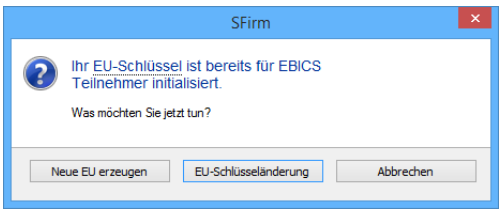
Anschließend ist der Status des EBICS-Teilnehmers in SFirm auf *INI/HIA* zu ändern. Öffnen Sie dazu den entsprechenden EBICS-Bankzugang über *Stammdaten ▸ Bankzugänge ▸ EBICS*. Im Reiter *EBICS Benutzer* markieren Sie den betreffenden Benutzer und klicken dann auf die Schaltfläche <Status>. Damit öffnet sich der Dialog *Teilnehmer Status*, wo Sie *initialisieren (INI/HIA)* auswählen (siehe auch Abschnitt Der Status des EBICS-Benutzers)



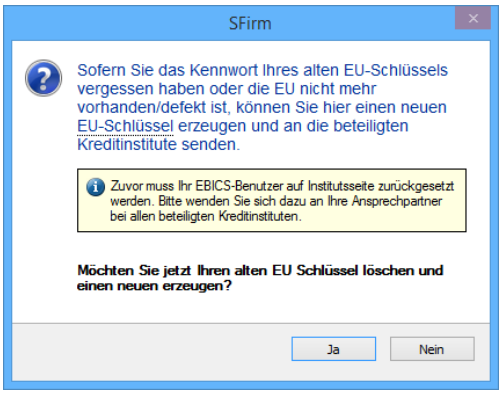
Rufen Sie die Funktion *EU Schlüssel erzeugen* in der EBICS-Schlüsselverwaltung (*Stammdaten ▸ Bankzugänge ▸ EBICS ▸ EBICS-Schlüsselverwaltung)* auf. Sie werden auf die Tatsache aufmerksam gemacht, dass bereits ein Schlüsselpaar vorhanden ist und mit einer Änderung weitere Schritte folgen müssen. Beantworten sie die Abfrage mit <Ja>.



Da bereits ein initialisierter EU-Schlüssel für den angemeldeten Teilnehmer existiert, werden Sie gefragt, ob Sie einen neuen Schlüssel erzeugen oder eine Schlüsseländerung durchführen möchten. Wählen Sie hier die <Neue EU erzeugen>.



Anschließend erscheint ein Hinweisdialog, welches Sie auf die Tatsache aufmerksam macht, dass das bereits vorhandene Schlüsselpaar gelöscht und ein neues erzeugt wird. Ist dies gewollt, beantworten sie die Abfrage mit <Ja>.



Der weitere Ablauf entspricht den Arbeitsschritten in dem Abschnitt Separate Benutzerinitialisierung für das EU-Schlüsselpaar.

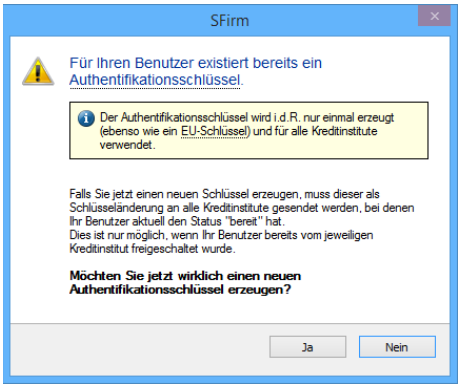
1.4 Änderung des Authentifikationsschlüssels

Möchten Sie einen vorhandenen Authentifikationsschlüssel ändern, dessen Kennwort noch bekannt ist, müssen Sie einen neuen Authentifikationsschlüssel erzeugen und an das Institut übertragen.

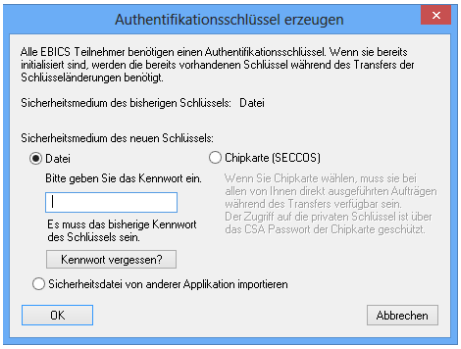
> Möchten Sie nur das Authentifikationskennwort ändern, kann dies jederzeit über die Schaltfläche <Authentifikationskennwort ändern> in der EBICS-Schlüsselverwaltung durchgeführt werden.

Rufen Sie die EBICS-Schlüsselverwaltung über das Menüband *Start ▸ EBICS-Schlüsselverwaltung,* innerhalb der *Bankzugänge* (EBICS) auf. Klicken Sie dort auf die Schaltfläche <Authentifikationsschlüssel erzeugen>.

Wird die Schaltfläche angeklickt wird zunächst eine Meldung angezeigt, die den Anwender über die Folgen dieser Aktion informiert.

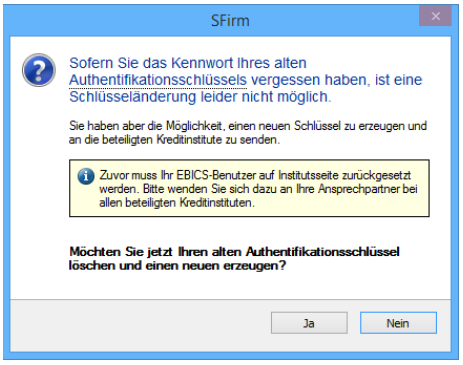


Existiert bereits für den aktuellen Teilnehmer ein Authentifikationsschlüssel (bzw. eine entsprechende .auth-Datei im Krypto-Ordner) und steht der Teilnehmer bei mindestens einem EBICS-Bankzugang im Status *bereit*, wird die Schaltfläche <Kennwort vergessen> eingeblendet. Damit kann der alte Authentifikationsschlüssel gelöscht und der Benutzer für alle EBICS-Bankzugänge automatisch auf den Status INI/HIA zurückgesetzt werden.



> Die Schaltfläche ist nicht bei der Auswahl von *Sicherheitsdatei von anderer Applikation importieren* oder *Chipkarte (SECCOS)* vorhanden.

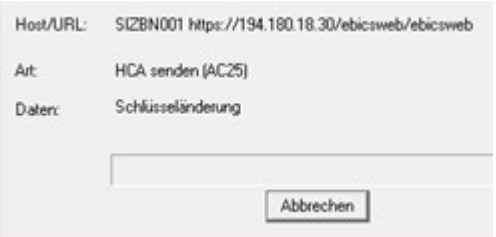
Wird die Sicherheitsabfrage bestätigt, wird die .auth-Datei gelöscht und der Status des EBICS-Teilnehmers von *bereit* auf *INI/HIA* gesetzt.



Nach der Bestätigung mit <OK> erhält der Teilnehmer bzw. Host in der Übersicht der Schlüsselverwaltung den Status *HCA*. Dieser gilt, wenn ein neuer Authentifikationsschlüssel erzeugt, aber noch nicht an das Institut gesendet wurde. Klicken Sie jetzt auf <Schlüssel senden>.

Stellen Sie nun das Sicherheitsmedium für die elektronische Unterschrift bereit und geben Sie das EU-Kennwort ein.

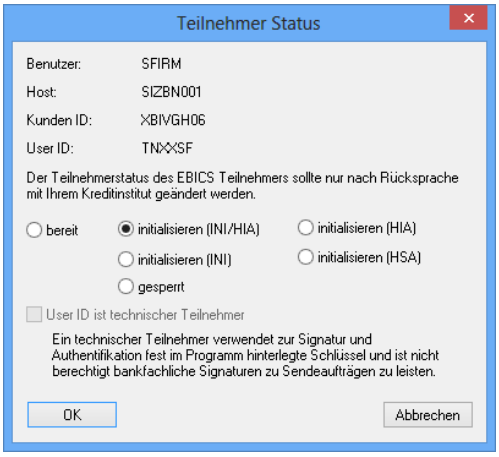
Es folgt nun ein EBICS-Transfer mit der Art *HCA senden*. Nach der Übertragung ist die Schlüsseländerung abgeschlossen.



1.4.1 Ersetzen des Authentifikationsschlüssels

Ist der Authentifikationsschlüssel und/oder das dazugehörige Kennwort nicht mehr vorhanden, muss der Teilnehmer zunächst auf Seiten des Rechenzentrums zurückgesetzt werden.

Zunächst ist der Status des EBICS-Teilnehmers in SFirm auf *INI/HIA* zu ändern. Öffnen Sie dazu den entsprechenden EBICS-Bankzugang über *Stammdaten ▸ Bankzugänge ▸ EBICS*. Im Reiter *EBICS Benutzer* klicken Sie auf die Schaltfläche <Status>. Damit öffnet sich der Dialog *Teilnehmer Status*, wo Sie *initialisieren (INI/HIA)* auswählen (siehe auch folgenden Abschnitt).



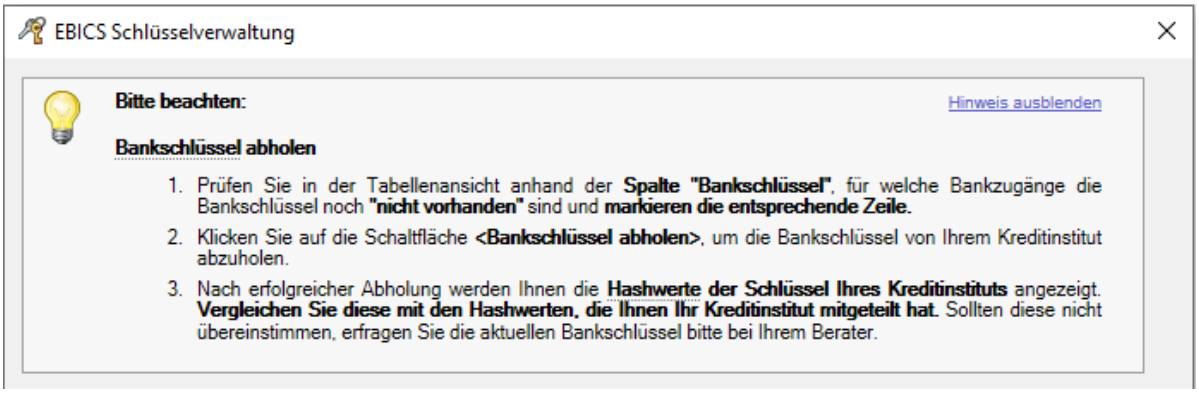
Löschen Sie anschließend über einen Dateimanager aus dem Unterordner Krypto die Datei [SFirm-Benutzername].auth. SFirm muss dazu nicht beendet werden. Beachten Sie bitte, nur die Datei zu löschen, deren Dateiname dem Benutzernamen des EBICS-Teilnehmers entspricht, dessen Authentifikationsschlüssel ersetzt werden soll.

1.5 Bankschlüssel abholen

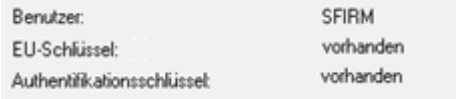
Das Abholen und Verifizieren eines Bankschlüssels ist obligatorisch. Ohne Bankschlüssel können keine Aufträge gesendet bzw. empfangen werden. Es muss nur einmal pro Host (Bankzugang) eine Abholung vorgenommen werden.

Beachten Sie außerdem, dass die Abholung des Bankschlüssels erst dann erfolgreich vorgenommen werden kann, wenn der Benutzer vollständig initialisiert bzw. auf Seiten des Bankrechners frei geschaltet wurde. Ist dies (noch) nicht der Fall, scheitert der Transfer. In den *anstehenden Aufgaben* werden Sie auf fehlende Bankschlüssel hingewiesen. Über diesen Hinweis gelangen Sie in die EBICS-Schlüsselverwaltung.

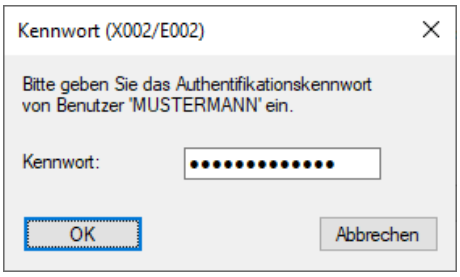
In der EBICS-Schlüsselverwaltung wird Ihnen nun das genaue Vorgehen zur Abholung der Bankschlüssel angezeigt:



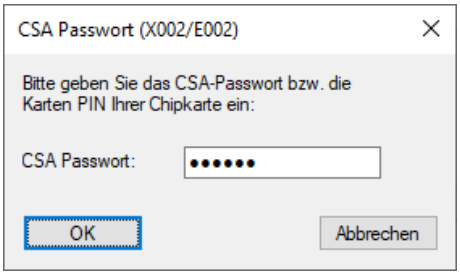
In der Übersicht der Schlüssel sehen Sie zum jetzigen Zeitpunkt jeweils den Status *vorhanden*.



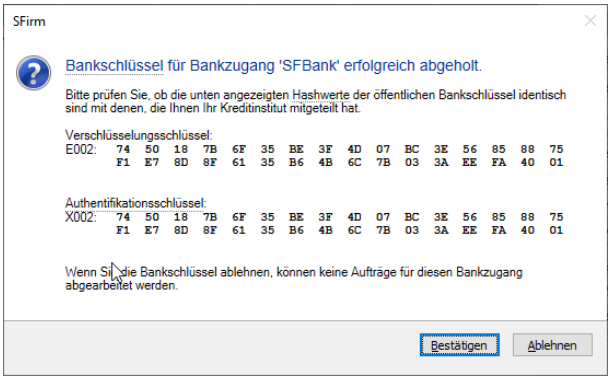
Bei dem EBICS-Bankzugang ist jetzt in der Spalte *Status* der Eintrag *bereit* zu sehen, bei *Bankschlüssel* steht *nicht vorhanden*. Klicken Sie nun auf die Schaltfläche <Bankschlüssel abholen>. Geben Sie hier das Kennwort zu Ihrem Authentifikationsschlüssel ein.



Ist das Sicherheitsmedium eine SECCOS-Chipkarte, werden Sie stattdessen aufgefordert, die Chipkarte einzulegen und das CSA-Passwort einzugeben.



Nach einer erfolgreichen Übertragung werden die Hash-Werte der öffentlichen Bankschlüssel angezeigt. Die angezeigten Hash-Werte müssen nun mit den Hash-Werten abgeglichen werden, die Ihnen vom Institut mitgeteilt wurden.



Ist der Abgleich korrekt, bestätigen Sie mit <Ja>. Bei <Nein> wird der Schlüssel verworfen und die Abholung muss zu einem anderen Zeitpunkt wiederholt werden.

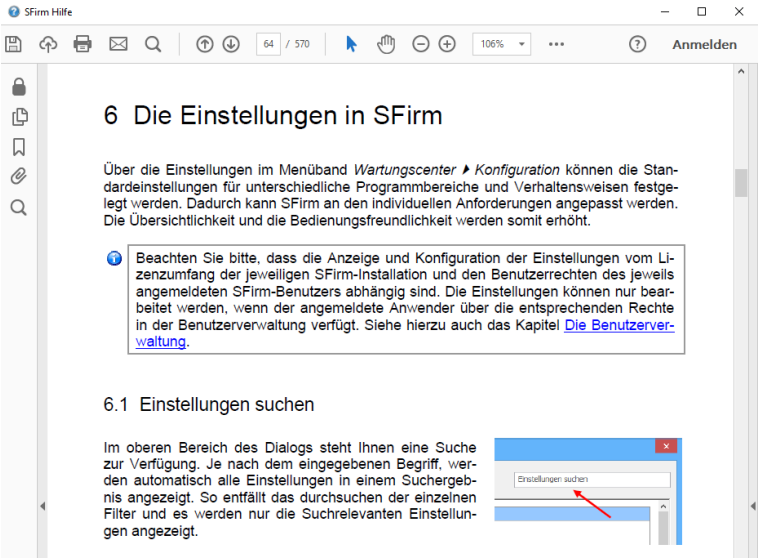
2 Weitere Informationsquellen & Support

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.

2.1 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.

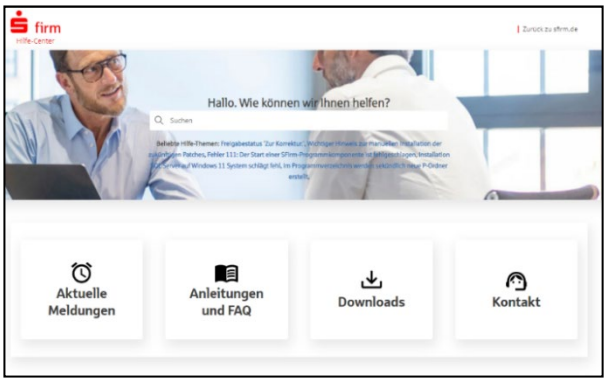


2.2 Der Internetauftritt von SFirm

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.

2.2.1 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.



2.2.2 Seminare

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

2.3 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).

2.4 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).