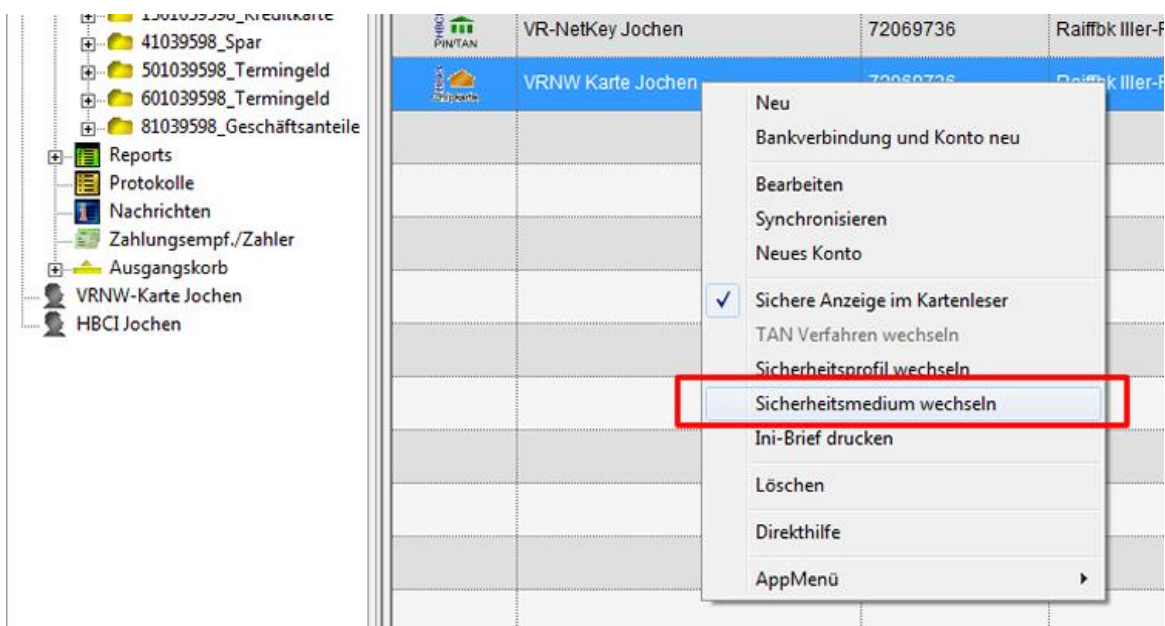


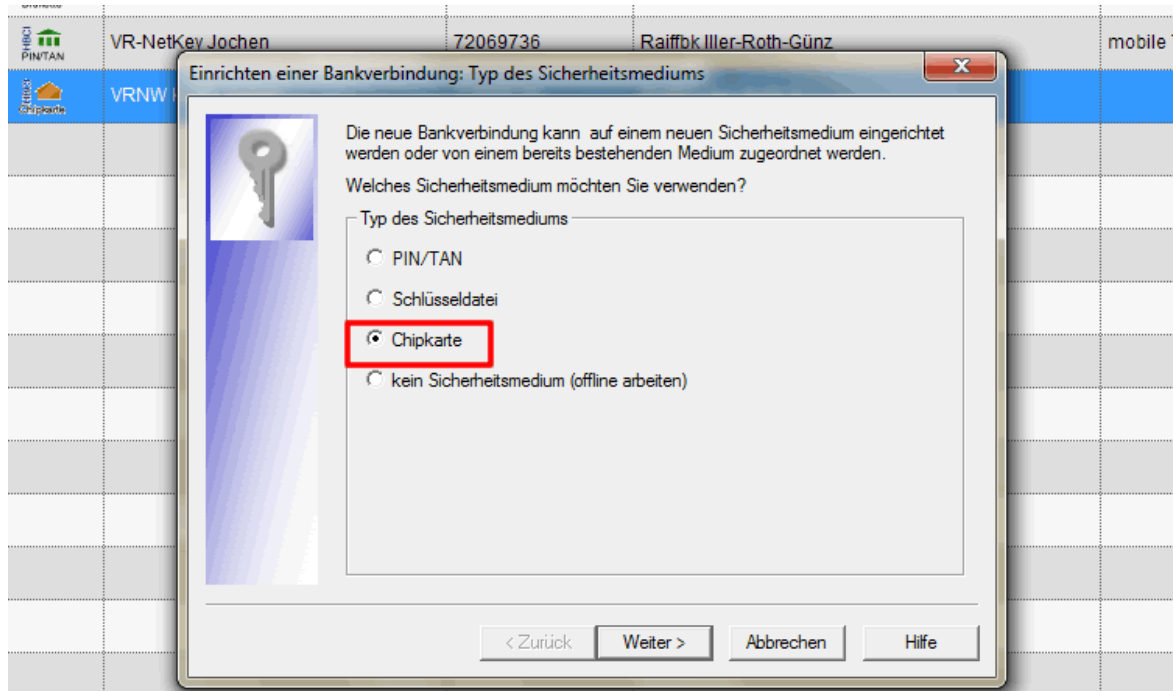
## Chipkarte – Sicherheitsmedium wechseln

Bei der Auslieferung einer neuen Chipkarte muss diese in der VR-NetWorld Software unter „Bankverbindungen“ aktiviert werden. Dabei gehen Sie wie folgt vor: Klicken Sie mit der rechten Maustaste auf die bestehende „Chipkarte, hier im Beispiel: VRNW Karte..“ und wählen Sie „Sicherheitsmedium wechseln“

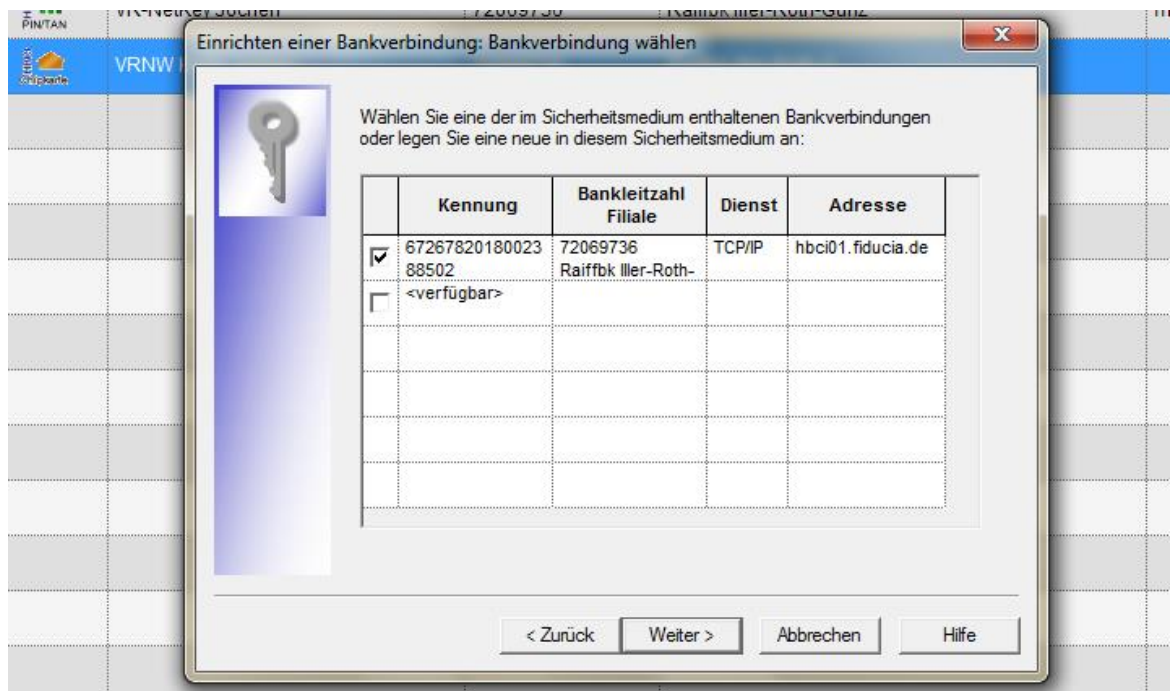


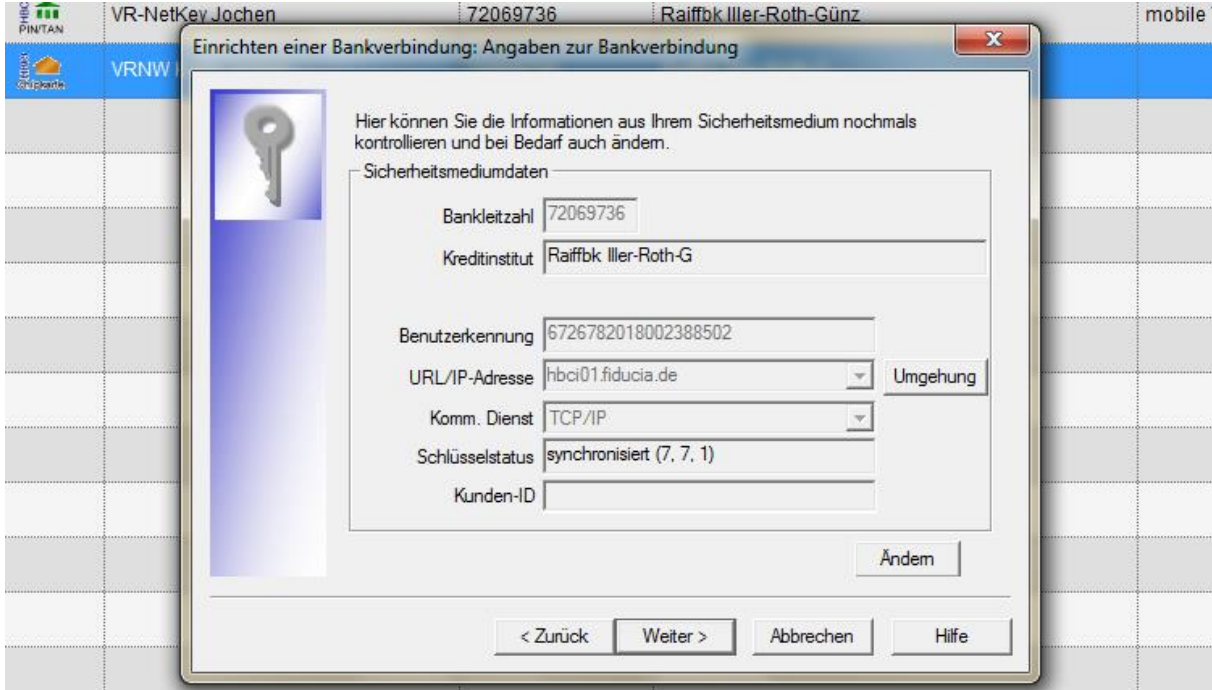
Bestätigen Sie folgende Meldung mit „Ja“

Wählen Sie „Chipkarte“



Bitte kontrollieren Sie, ob der Haken bei Bankverbindung gesetzt ist.





Einrichten einer Bankverbindung: Angaben zur Bankverbindung

Hier können Sie die Informationen aus Ihrem Sicherheitsmedium nochmals kontrollieren und bei Bedarf auch ändern.

Sicherheitsmediumdaten

Bankleitzahl

Kreditinstitut

Benutzerkennung

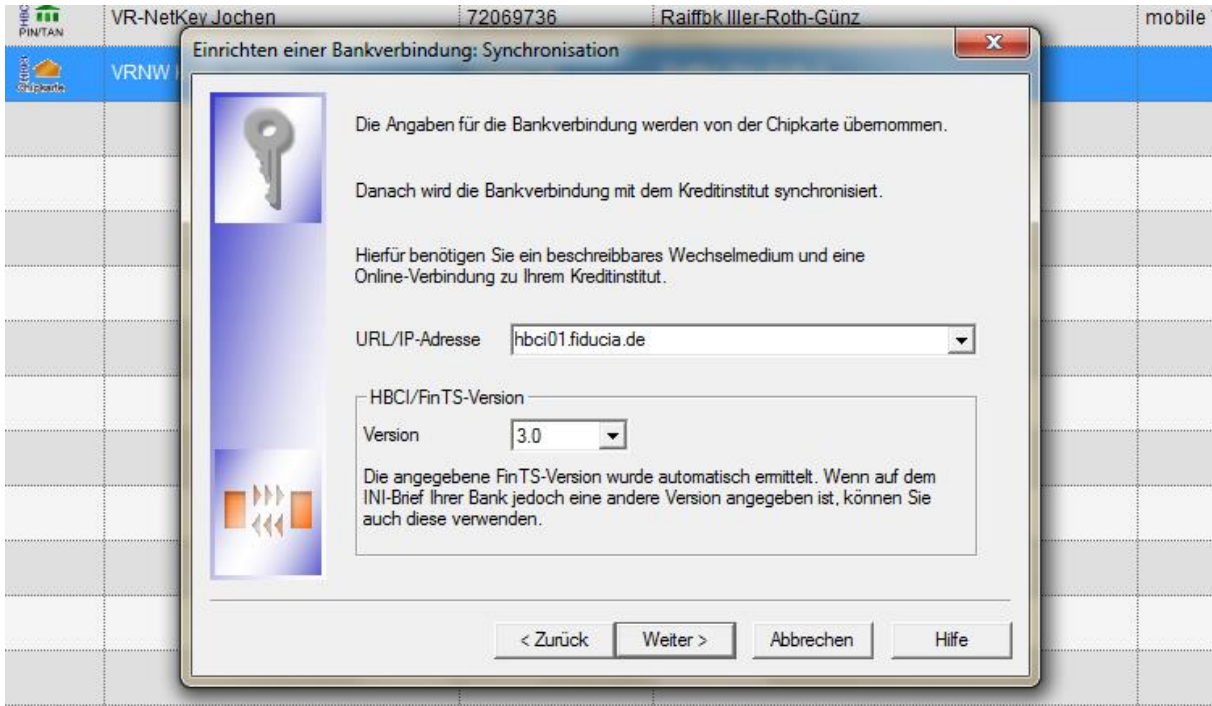
URL/IP-Adresse

Komm. Dienst

Schlüsselstatus

Kunden-ID

Anschließend richten Sie die Bankverbindung ein, und kontrollieren Sie die Angaben.  
Bitte mit **Weiter** bestätigen



Einrichten einer Bankverbindung: Synchronisation

Die Angaben für die Bankverbindung werden von der Chipkarte übernommen.

Danach wird die Bankverbindung mit dem Kreditinstitut synchronisiert.

Hierfür benötigen Sie ein beschreibbares Wechselmedium und eine Online-Verbindung zu Ihrem Kreditinstitut.

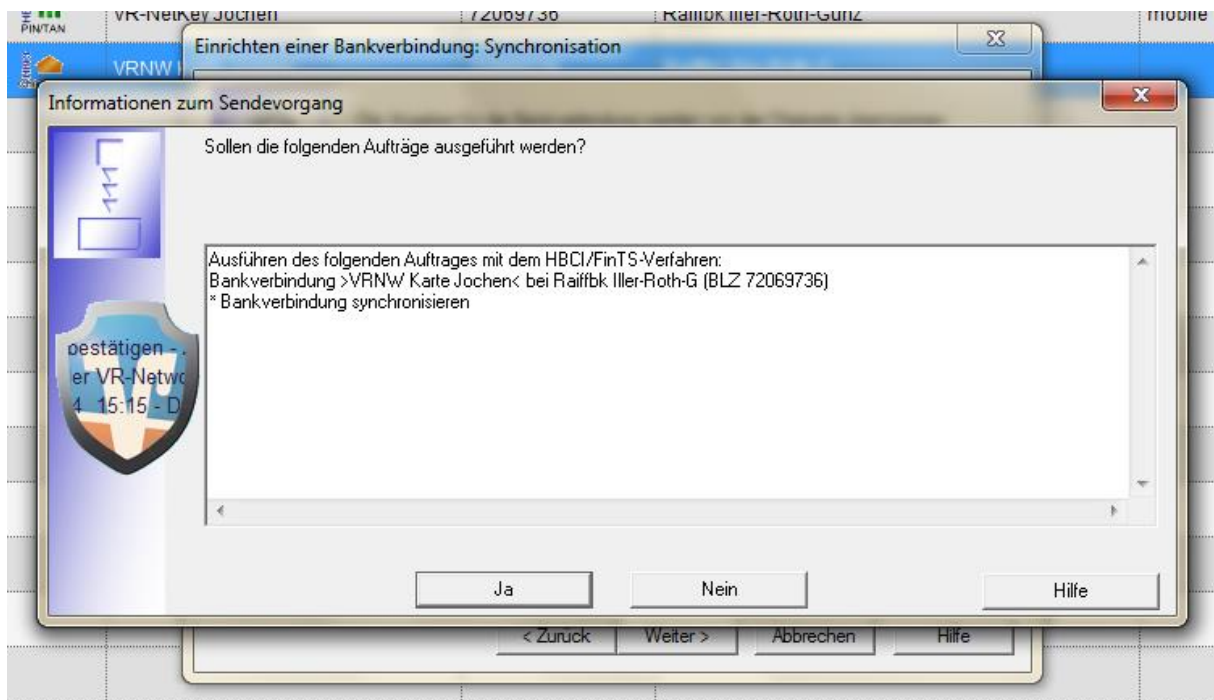
URL/IP-Adresse

HBCI/FinTS-Version

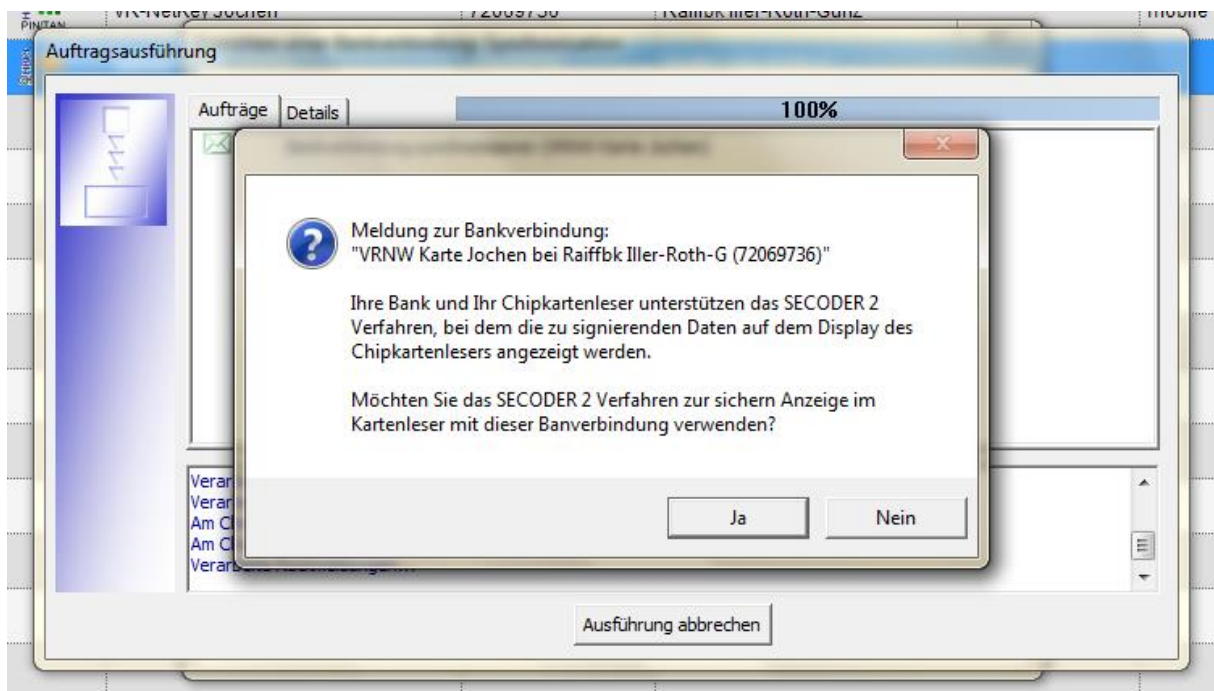
Version

Die angegebene FinTS-Version wurde automatisch ermittelt. Wenn auf dem INI-Brief Ihrer Bank jedoch eine andere Version angegeben ist, können Sie auch diese verwenden.

Bitte mit **Weiter** bestätigen



Bitte mit **Ja** bestätigen



Wenn Sie hier mit **Ja** bestätigen, wird der Ablauf dem SECODER 2\* - Verfahren angepasst.

Wenn Sie hier mit **Nein** bestätigen, so funktioniert der Autorisierungsvorgang bei einer Transaktion wie bisher.

Danach können Sie die Bankverbindung synchronisieren und ggf. Konten hinzufügen.

**\*Der Secoder Standard:**

Der Secoder Standard zeichnet sich durch besondere Sicherheitsmerkmale aus, die ihn von herkömmlichen Kartenlesern unterscheiden: Er verfügt über eine eingebaute Firewall, die die Karte und die Geheimzahl des Nutzers schützt, sowie ein Display, welches die Transaktionsdaten zur Kontrolle anzeigt, womit jede Manipulation auffällig wird. Die Secoder-Erweiterung für HBCI erlaubt etwa die manipulationssichere Anzeige der Überweisungsdaten (Zahlungsempfänger und Betrag) im Gerätedisplay. Diese muss allerdings von der jeweiligen Bank aktiv unterstützt werden. Außerdem ist die Eingabe der PIN auf dem Lesegerät zwingend. Angriffsversuche durch Schadsoftware wie Trojaner oder Keylogger soll der Secoder durch die Firewall abwehren, wodurch die Anwendungssoftware selbst keinen unmittelbaren Zugriff auf das Gerät erhält. Da der Secoder-Standard zwingend Tastatur und Display vorsieht, entsprechen derartige Kartenleser immer auch mindestens der Sicherheitsklasse 3.

**Was ist neu mit dem Secoder 2 Verfahren?**

Bei dem Secoder 2-Verfahren akzeptiert der Leser zusätzlich nur zertifizierte Softwareupdates. Ein Nutzer kann also sicher sein, dass nur die angezeigte Transaktion von ihm freigegeben wird und ihm ein Hacker somit keine anderen Daten unterschiebt. Das patentierte Secoder 2-Verfahren ist der höchste Sicherheitsstandard der Deutschen Kreditwirtschaft für Chipkartenleser und Transaktionsabsicherung