MVSC - Multivia Sm@rtConnect

Anwenderdokumentation

ATRUVIA

Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken

MVSC - Multivia Sm@rtConnect

Anwenderdokumentation

Version: 4.5
Datum/Uhrzeit: 29.10.2025 / 11:32 Uhr

Gegenüber der vorherigen Ausgabe wurden folgende Änderungen vorgenommen:

Nummer	Datum	Inhalt / Änderungen
12	13.10.2025	Ergänzung zum MVSC-Release 4.5: • Das Kapitel "Nutzung" wurde in "Nutzung von MVSC" umbenannt und um das neue Unterkapitel "Empfängerprüfung" erweitert.
11	17.10.2024	Ergänzung zum MVSC-Release 4.0: • In die "Einleitung" in den Abschnitt "Generelle Nutzbarkeit MVSC", "Kurzbeschreibung MVSC" wurde eine Beschreibung zur Nutzung der Java-Version 1.8 oder der Java-Version 17 aufgenommen. Dafür wurden auch zwei Web-Adressen zum Herunterladen der jeweils zu verwendenden MVSC-Version ergänzt. • In dem Kapitel "Nutzung in der Konsole" im Abschnitt "Aufruf aus der Konsole" wurde die Aufrufvariante "D" in Abschnitte für Upload - und für Download-Auftragsarten aufgeteilt. Die Beschreibung für Download-Auftragsarten wurde neu aufgenommen.
10	28.08.2023	Ergänzung zum MVSC-Release 3.5.0: • Im Abschnitt "Legitimation" des Kapitels "Einrichtung", "Programmstart" wurde die Notwendigkeit der Änderung des Startpasswortes nach der ersten Anmeldung beschrieben.
09	16.11.2022	Ergänzung zum MVSC-Release 3.0.0: • Das Kapitel "Technisches Logging" wurde angepasst: Die Abbildung des Menuepunkts "Hilfe", "Logging" wurde erneuert und in den Abschnitt "Log-Level" verschoben. Der Abschnitt "Menuepunkt" ist damit entfallen. • In dem Kapitel "Hilfe" wird nun auf das Handbuch verwiesen. Die Beschreibung der "Hilfetexte" ist entfallen.

Nummer	Datum	Inhalt / Änderungen
08	13.05.2022	Ergänzung zum MVSC-Release 3.0.0: • Das Kapitel "Struktur des Programms" wurde um den neuen Reiter "Auftragshistorie" erweitert. Zusätzlich wurde der Reiter "Konfiguration" in "Zugänge" umbenannt, um Verwechslungen mit dem gleichnamigen Menüpunkt "Konfiguration" zu vermeiden. • Das Kapitel "EBICS-Zugangsdaten erfassen" wurde im Abschnitt "Anlagevorgang" um die Beschreibung des empfohlenen Signaturmediums "Zertifikat" erweitert. Zudem wurden Hinweise aufgenommen, dass ab EBICS 3.0 keine neuen Chipkarten oder Sicherheitsdateien mehr generiert oder initialisiert werden können. • Das Kapitel "EBICS-Zugangsdaten erfassen" wurde um den Abschnitt "Schlüssel ändern" erweitert. • Das Kapitel "Kontrollmöglichkeiten" wurde um den neuen Abschnitt "Auftragshistorie" erweitert. • In dem Kapitel "Unterstützte Signaturverfahren" wurde im Abschnitt "Sicherheitsdatei" der Hinweis zur falschen Passworteingabe korrigiert. • In den Kapiteln "Nutzung in der Konsole", "Automatisierte Nutzung mit Hilfe einer Batch-Datei" und "Container-Erstellung" wurden die Aufrufvarianten von MVSC überarbeitet.
07	11.03.2021	Ergänzung zum MVSC-Release 2.6.0: • In das Kapitel "Generelle Nutzbarkeit MVSC" der "Einleitung" wurde eine kurze Beschreibung des Unterschieds zwischen der "MVSC Vollversion" und "MVSC Sign" aufgenommen. • In das Kapitel "Struktur des Programms" wurde ein Hinweis auf "MVSC Sign" aufgenommen.
06	04.03.2020	Ergänzung zum MVSC-Release 2.6.0: • In den Abschnitt "Upload-Auftragsart ausführen" des Kapitels "Datenübertragung im Dialog" wurde ein Tipp zur Nutzung der Auftragsart "AUTO" aufgenommen. • Das Kapitel "Nutzung in der Konsole" wurde um den Abschnitt "Auftragsarten 'AUTO' und 'AUTD'" erweitert.
05	06.08.2019	Ergänzung zum MVSC-Release 2.5.0: • Die Einleitung wurde um den neuen Abschnitt "Mehrsprachigkeit" erweitert. • In das Kapitel "Unterstützte Signaturverfahren" wurde in den Abschnitt "Sicherheitsdatei" ein Hinweis zur 5-maligen falschen Passworteingabe aufgenommen. • Das Kapitel "Verzeichnisstruktur" wurde um den Ordner "Original" erweitert. • Im Kapitel "Installation" wurde der Abschnitt "Update der Signaturversion einer Zugangs-ID" neu aufgenommen. Außerdem wurde die Auswahl der Defaultsprache im Abschnitt "Installation mit dem Assistenten 'install.jar'" ergänzt. • Im Kapitel "EBICS-Zugangsdaten erfassen" wurde im Abschnitt "Anlagevorgang" die Möglichkeit der Vergabe der Zugangs-ID um die Angaben der zulässigen Zeichen und Länge ergänzt. Außerdem wurden einige Screenshots ausgetauscht, da sich die Reihenfolge der Auswahlmöglichkeiten für die Signaturversion geändert hat. • In den Abschnitt "Gruppierung 'Sonstige Einstellungen'" des Kapitels "Vorbelegungen" wurde die neue Option "Ausgewählte Sepa-Dateien als IBAN-Only senden" aufgenommen.
04	11.10.2018	Ergänzung zum MVSC-Release 2.0.3: • Kapitel "Generelle Nutzbarkeit MVSC" und Kapitel "Systemvoraussetzungen": Es ist eine Java-Version 1.7 oder 1.8 erforderlich.

Öffentlich (C1)

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Einleitung

1. Generelle Nutzbarkeit MVSC

Kurzbeschreibung MVSC

MVSC ist ein auf Java basierendes Tool zur sicheren Übertragung von bereits erstellten Auftragsdateien über das EBICS-Verfahren. Das Programm lässt sich in den zwei verschiedenen Modi "Benutzeroberfläche" und "Konsolenaufruf" ausführen, die es ermöglichen, die Software bedarfsgerecht abzustimmen.

"MVSC Sign" unterscheidet sich zudem von der "MVSC Vollversion" darin, dass mit "MVSC-Sign" Auftragsdateien nur unterschrieben werden können. Das Senden und Abholen von Auftragsdateien ist dagegen mit "MVSC-Sign" nicht möglich. Der Reiter "Datenübertragungen" steht Ihnen nur in der "MVSC Vollversion" und nicht in "MVSC Sign" zur Verfügung.

MVSC profitiert von der in JAVA gegebenen Plattformunabhängigkeit und kann auf allen Betriebssystemen ausgeführt werden, auf denen eine JAVA-Version 1.8 oder 17 installiert ist.

Es gibt 2 Versionen von MVSC, einmal für Java 1.8 und einmal für Java 17, daher gibt es auch zwei Web-Adressen zum Herunterladen der Version von MVSC.

Wenn Sie die MVSC-Version für **Java 1.8** verwenden möchten, so rufen Sie die folgende Web-Adresse auf:

"https://smartconnect.multivia-suite.de/software/Install_MVSC.jar".

Wenn Sie die MVSC-Version für **Java 17** verwenden möchten, so rufen Sie die folgende Web-Adresse auf:

https://smartconnect.multivia-suite.de/software/Install_MVSC17.jar

Anmerkung: Updates werden automatisch eingespielt, wenn die jeweilige MVSC-Version bereits vorliegt.

Mehrsprachigkeit

Im rechten oberen Bereich stehen Ihnen Schaltflächen zur Auswahl der Sprache zur Verfügung.

Dies ist in der folgenden Abbildung dargestellt:

Abb. 1. Spachauswahl im rechten oberen Bereich

2. Grundlagen EBICS

Definition

Die Abkürzung EBICS (Electronic Banking Internet Communication Standard) bezeichnet einen multibankfähigen Standard zur Übertragung von Zahlungsverkehrsdateien über die Internetprotokolle TCP/IP, HTTP und HTTPS. EBICS gilt als Nachfolger des zuvor am Markt existierenden FTAM-Standards "DFÜ mit Kunden", der per Direkteinwahl über ISDN bzw. DATEX-P mit dem Bankrechner kommunizierte.

Sicherheitsaspekte

Es wurde an vielen Merkmalen FTAM's festgehalten, wie zum Beispiel am Datenmodell (Kunde/ Teilnehmer/ Konto) und am Freischaltungsverfahren (INI-Brief). Die elektronische Unterschrift aus FTAM wird in EBICS ebenfalls unterstützt. Ein Umstieg für bisherige FTAM-Kunden auf das neue EBICS-Verfahren ist somit möglich. Neben der bisher in FTAM unterstützten elektronischen Unterschrift, die in Form einer Sicherheitsdatei aufbewahrt wird, gibt es in EBICS zusätzlich die Möglichkeit, die elektronische Unterschrift auf einer Chipkarte aufzubewahren. Näheres zur Einrichtung eines EBICS-Zugangs unter MVSC erfahren Sie im Kapitel "Einrichtung".

Gesetzliche Regelungen

Seit dem 1. Januar 2008 besteht eine bankseitige Verpflichtung zur Unterstützung des EBICS-Standards, während dieselbe Verpflichtung für das FTAM-Verfahren am 31.10.2010 endete. (http://www.ebics-zka.de/).

1. Funktionalitäten

1.1. Allgemeines zur Funktionalität

Aufrufvarianten

Die Benutzeroberfläche von MVSC bietet Ihnen alle benötigten Funktionen,- diese reichen von der Erfassung der EBICS- bzw. Internet-Verbindungsdaten bis hin zu Datenübertragungen jeglicher Art.

Wurde der EBICS-Zugang einmalig über die Benutzeroberfläche in Betrieb genommen, so ist die Nutzung des Konsolenmodus nur noch eine Frage des Programmaufrufs.

1.2. Unterstützte Signaturverfahren

Signaturverfahren

EBICS bietet die Signaturverfahren "Sicherheitsdatei" und "Chipkarte". MVSC unterstützt beide Verfahren sowie alle bislang existierenden Signaturversionen (A004/ A005/ A006) bzw. Schlüssellängen.

Anmerkung
Für den Einsatz der Chipkarte wird entsprechende Hardware benötigt (Chipkartenleser/ Signaturkarten).

Sicherheitsdatei

Die Erstellung einer eigenen, passwortgeschützten Sicherheitsdatei erfolgt durch eine in MVSC vorhandene Funktionalität. Der Aufbewahrungsort für die physikalische Sicherheitsdatei und des dazugehörigen Passworts sollte aus Sicherheitsgründen nicht unmittelbar beieinander liegen, da trotz verschlüsselter Ablage in MVSC ein Restrisiko besteht.

Tipp
Legen Sie Ihre Sicherheitsdatei auf einem USB-Stick ab.

Achtung
Bei 6-maliger falscher Passworteingabe werden der Zugang und die Sicherheitsdatei unwiderruflich gelöscht.

Chipkarte

Sofern Sie eine EBICS-fähige Chipkarte besitzen, empfehlen wir, diese anstelle einer Sicherheitsdatei zu verwenden. Chipkarten bieten generell eine höhere Sicherheit, da die darauf gespeicherten privaten Schlüssel niemals auf einer Festplatte oder ähnlichem abgelegt werden können. Die auf einer Chipkarte enthaltenen Schlüssel zur Signatur und Verschlüsselung sind durch zwei PINs (Karten- und Signatur-PIN) gesichert. Diese können jedoch auch gleich sein. Die Eingabe der PINs erfolgt über die Tastatur eines entsprechenden Chipkartenlesers. Das bietet gegenüber der Passworteingabe über die gewöhnliche Tastatur eine zusätzliche Sicherheit vor Angriffen durch bösartige Software (z.B. Trojanische Pferde).

Achtung
Sollten Sie im Besitz einer personalisierten Chipkarte sein, stellen Sie sicher, dass Ihnen die PINs der Karte bekannt sind. Wurden diese noch nicht geändert, so entnehmen Sie die initialen PINs Ihren PIN-Briefen.

Anmerkung
Das Signaturverfahren "Chipkarte" ist nicht für die automatisierte Datenübertragung geeignet. Sollen bestimmte Zugangsdaten im Konsolenmodus nutzbar sein, muss als Signaturverfahren die "Sicherheitsdatei" ausgewählt werden.

1.3. Unterstützte Auftragsarten

Allgemeines

Die Anwendung MVSC unterstützt alle in EBICS vorgesehenen Auftragsarten. Im Programm werden jedoch nur die Auftragsarten angezeigt, die für den jeweiligen Zugang am EBICS-Server administriert bzw. zugeordnet wurden.

Auftragsarten synchronisieren

Sollten zusätzliche Auftragsarten benötigt werden, so müssen diese am EBICS-Server freigeschaltet werden. Anschließend sind die in MVSC bekannten Auftragsarten erneut mit dem Bankrechnersystem zu synchronisieren.

Verteilte elektronische Unterschrift ("VEU")

Bei der "VEU" handelt es sich um ein standortunabhängiges Freigabesystem für Aufträge. Das bedeutet, wenn der Teilnehmer X eines Kunden nicht ausreichend berechtigt ist, eine Auftragsart mit seiner alleinigen Unterschrift auszuführen, gelangt der Auftrag in einen sogenannten "Auftragspool". Andere für dieses Konto berechtigte Teilnehmer (Y) haben nun die Möglichkeit, sich eine Übersicht der dort gesammelten Aufträge abzuholen. Wurde die Übersicht erfolgreich abgeholt, so kann Teilnehmer Y die auf Unterschrift wartenden Aufträge einsehen und anschließend ebenfalls unterschreiben bzw. stornieren.

1.4. Verwaltung von Zugangs- und Verbindungsinformationen

EBICS

Zur Erfassung eines funktionstüchtigen EBICS-Zugangs benötigen Sie die folgenden Informationen von Ihrem BPD-Blatt:

- Kunden-ID
- Hostname des EBICS-Servers (8-stellig)
- URL des EBICS-Servers (beginnend mit "https")
- Teilnehmer-ID
- EBICS-Version (Unterstützte Versionen können über eine Schaltfläche abgerufen werden.)

Wurden diese Daten in der Benutzeroberfläche eingegeben und gespeichert, ist anschließend das Sicherheitsmedium zu konfigurieren:

- Signaturmedium
- Signaturversion (muss bei Verwendung eines bestehenden Mediums bekannt sein)
- Pfad der Sicherheitsdatei/ Kartennummer (Schaltfläche "Karte zuordnen")
- ggf. Passwort für die Sicherheitsdatei (Nutzung im Konsolenmodus)

Internet

Falls eine direkte Verbindung zum Internet besteht, sind keine Änderungen an der voreingestellten Verbindungsart notwendig. Sollte die Verbindung über einen Proxy-Server hergestellt werden, so lassen sich auch diese Einstellungen einfach hinterlegen.

1.5. Struktur des Programms

Menüpunkte

Nachdem sich der Benutzer über die Anmeldemaske erfolgreich am Programm authentifiziert hat, öffnet sich das Hauptfenster der Anwendung.

Dabei stehen Ihnen die in der folgenden Abbildung dargestellten Reiter zur Verfügung:

Abb. 1.1. Reiter des Hauptfensters der Anwendung

In der folgenden Tabelle werden die einzelnen Reiter erläutert:

Reiter	Funktionalität / Beschreibung
Datenübertragungen	Diese Maske bietet die Möglichkeit, Datenübertragungen durchzuführen. Dazu wählen Sie den jeweiligen EBICS-Zugang aus und bestimmen anschließend die gewünschte Auftragsart und die zu übertragenden Dateien. Die Ausführung von Aufträgen ist erst möglich, wenn Ihre EBICS-Zugangsdaten vollständig im Programm erfasst und am EBICS-Bankrechner initialisiert wurden. **Anmerkung** Dieser Reiter "Datenübertragungen" steht Ihnen nur in der "MVSC Vollversion" und nicht in "MVSC Sign" zur Verfügung.
Auftragshistorie	Hier haben Sie die Möglichkeit, sich die Einträge aus dem HAC-Protokoll anzeigen zu lassen. Dabei werden Ihnen alle Aufträge angezeigt, die sich auf die jeweilige Kunden-ID und die jeweilige Zugangs-ID beziehen. **Tipp** Unter dem Menüpunkt "Konfiguration"->"Einstellungen" können Sie festlegen, wie lange die Einträge in der Auftragshistorie angezeigt werden. Näheres dazu finden Sie im Abschnitt "Auftragshistorie" des Kapitels "Kontrollmöglichkeiten".
Unterschriften	Das EBICS-Verfahren bietet die Möglichkeit, Aufträge im 4-Augen-Prinzip freizugeben. Die noch nicht vollständig autorisierten Aufträge werden dann am EBICS-Bankrechner abgelegt und warten auf weitere Unterschriften durch berechtigte Teilnehmer. Erst wenn eine oder mehrere weitere Unterschriften geleistet wurden, wird der Auftrag an die verarbeitenden Systeme weitergegeben. Die Übersicht der auf Unterschrift wartenden Aufträge kann unter Angabe des EBICS-Zugangs unter diesem Reiter aufgerufen werden. Die Aufträge können unterschrieben oder auch storniert werden.
Zugänge	Unter diesem Reiter befinden sich alle Eingabefelder zur Erfassung von EBICS-Zugangsdaten. Hier sind die Zugangsinformationen zu erfassen. Die Konfiguration dient außerdem zum Erstellen bzw. Initialisieren der zugehörigen Sicherheitsmedien. Auch die am System hinterlegten Auftragsarten können aus dieser Maske heraus abgerufen werden. Soll MVSC im Konsolenmodus genutzt werden, so können hier die notwendigen Vorbelegungen für den Aufruf angegeben werden.
Benutzer	Dieser Reiter dient zur Verwaltung der in MVSC hinterlegten Benutzer. Der Administrator hat das Recht, neue Benutzer anzulegen, zu löschen oder auch das Passwort anderer Benutzer zurückzusetzen. Alle anderen Benutzer können hier lediglich Ihr eigenes Passwort ändern.
Internet	Unter diesem Reiter kann die genutzte Internetverbindung hinterlegt werden. Diese Einstellung ist für alle angelegten Zugangs-IDs gültig. Sofern die Verbindung nicht über einen Proxy-Server hergestellt wird, können die Einstellungen unverändert bleiben. Andernfalls sind hier die Verbindungsdaten des verwendeten Proxy-Servers zu erfassen.
Logbuch	Die vom Anwender durchgeführten Aktionen werden protokolliert und in einer Log-Datei gespeichert. Für jeden Tag wird eine eigene Datei erzeugt. Der Reiter "Logbuch" bietet die Möglichkeit, diese Dateien einzusehen und zu filtern.

2. Technische Aspekte

2.1. Systemvoraussetzungen

Betriebssystem und Java-Umgebung

Sie benötigen eine Java-Laufzeitumgebung (JRE) der Version 1.7 oder 1.8, um MVSC auf Ihrem Computer nutzen zu können. MVSC ist dank seiner flexiblen Struktur kompatibel zu allen Betriebssystemen, die diesen JAVA-Standard unterstützen (z.B. Windows, Unix, Linux).

2.2. Verzeichnisstruktur

Inhalt des Programmverzeichnisses

Nachdem MVSC installiert wurde, befindet sich die in der folgenden Abbildung dargestellte Verzeichnisstruktur im angegebenen MVSC-Programmverzeichnis:

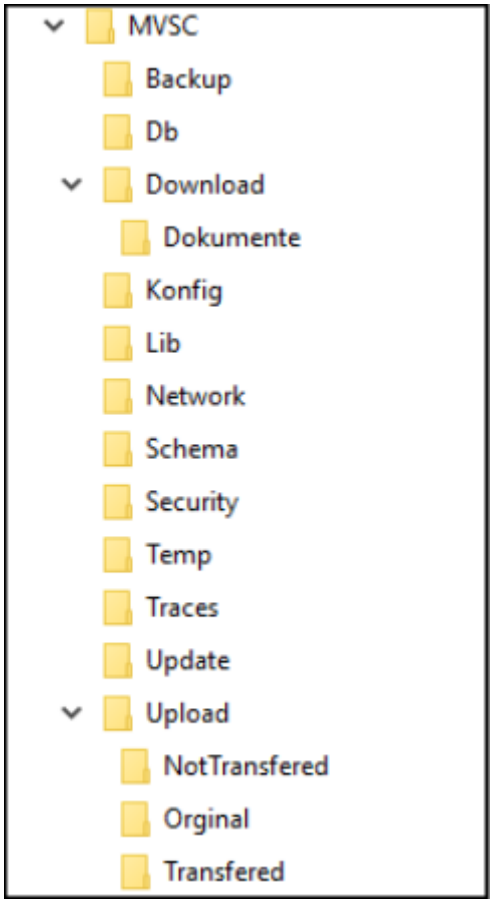


Abb. 2.1. MVSC-Verzeichnisstruktur

Up- und Download-Verzeichnis

Die Verzeichnisse "Download" und "Upload" gelten als Standardeingangspfad bzw. Standardausgangspfad für empfangene bzw. zur Übertragung vorgesehene Dateien. Beide Verzeichnisse lassen sich je Zugangs-ID beliebig konfigurieren. Unterhalb dieser Verzeichnisse befinden sich noch weitere Unterverzeichnisse ("Dokumente" bzw. "NotTransfered", "Original" und "Transfered").

Dokumentenablage

Das Verzeichnis "Dokumente" dient als Ablageort für empfangene Protokolldateien (Auftragsarten "PTK" und "HAC") und INI-Briefe. Um Dokumente von Auftragsdateien zu trennen, befindet es sich üblicherweise unterhalb des angegebenen Downloadpfads.

Auch dieses Verzeichnis ist je Zugangs-ID konfigurierbar. Nähere Informationen dazu finden Sie im Kapitel "Vorbelegungen".

Verarbeitete Dateien

Als Ablageort für übertragene Dateien dient der Ordner "Transfered" unterhalb des Upload-Verzeichnisses. Dieser Pfad kann ebenfalls je Zugangs-ID beliebig festgelegt werden. Die Trennung von bereits übertragenen und noch zur Übertragung anstehenden Dateien ist notwendig, da sonst im Konsolenmodus unter Umständen die gleichen Dateien mehrmals übertragen werden. Wenn im Konsolenmodus eine Datenübertragung fehlschlägt, wird die betroffene Datei in das "NotTransfered"-Verzeichnis verschoben. Im Oberflächenmodus hat das Verzeichnis "NotTransfered" keine Relevanz.

Das Verzeichnis "Original" dient zur Ablage der Originaldatei bei Verwendung der Option "Ausgewählte SEPA-Dateien als IBAN-Only senden". Näheres dazu finden Sie im Kapitel "Vorbelegungen" im Abschnitt "Gruppierung 'Sonstige Einstellungen'".

Sicherheitsdateien

Im Security-Verzeichnis bewahrt MVSC die generierten Sicherheitsdateien (*.ESK) auf. Außerdem werden hier die öffentlichen Schlüssel der verschiedenen EBICS-Bankrechner abgelegt (*.PKD).

Log- und Tracedateien

Technische Protokollierungsdateien, die uns als Hersteller im Fehlerfall weiterhelfen könnten, finden Sie im Verzeichnis Traces. Seit Version 2.0 werden hier auch die tageweise geschriebenen Aktionsprotokolle abgelegt.

Konfigurationsdateien (gültig bis MVSC-Version 2.0)

Alle erfassten Konfigurationsdaten befinden sich im Konfig-Verzeichnis. Dazu zählen angelegte Zugangs-IDs, Dateifiltereinstellungen, zugelassene Auftragsarten sowie die Internetverbindungsdaten.

Datenbankverzeichnis (gültig ab MVSC-Version 2.0)

Alle erfassten Konfigurationsdaten befinden sich ab der MVSC-Version 2.0 im DB-Verzeichnis in einer verschlüsselten Datenbank. Dazu zählen angelegte Zugangs-IDs, Dateifiltereinstellungen, zugelassene Auftragsarten sowie die Internetverbindungsdaten. Beim Update der MVSC-Version 1.0 auf 2.0 werden die Daten aus dem Konfig-Verzeichnis automatisch in die Datenbank importiert.

Sonstige Verzeichnisse

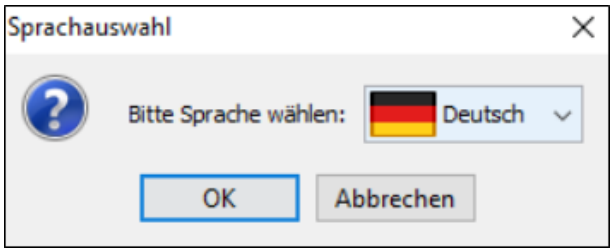
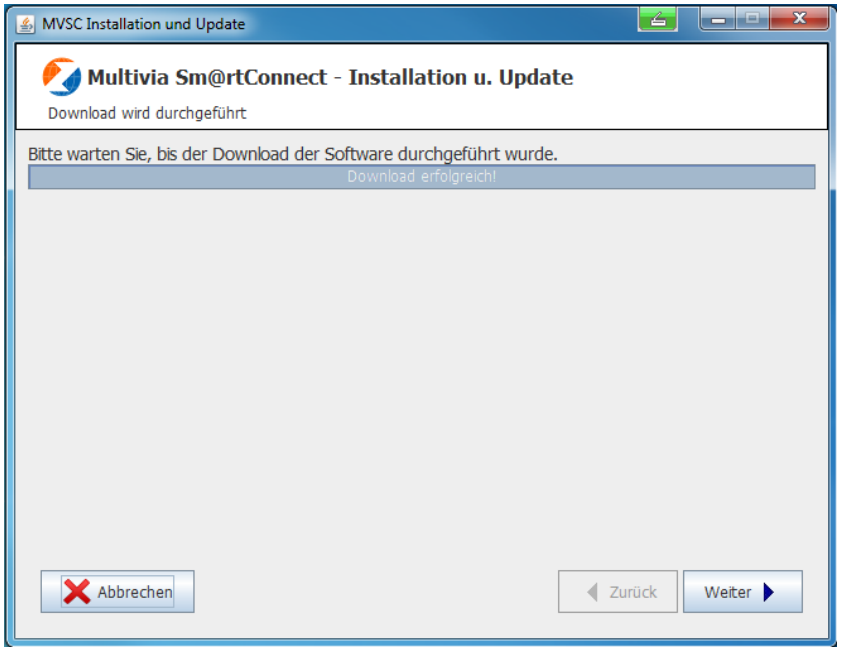
Die Verzeichnisse "Lib", "Temp" und "Network" sind für die Bedienung des Programms nicht relevant. Allerdings ist ohne die im Lib-Verzeichnis enthaltenen Dateien keine Datenübertragung via EBICS möglich. Wird eine Programm-Aktualisierung durchgeführt, so wird das zu installierende Update-Paket zunächst im Ordner "Update" gespeichert. Im Verzeichnis "Backup" werden vor der Durchführung einer Aktualisierung die wichtigsten Dateien gesichert. Die für die Validierung von SEPA-XML-Dateien notwendigen XML-Schema-Dateien (*.XSD) befinden sich im Verzeichnis "Schema".

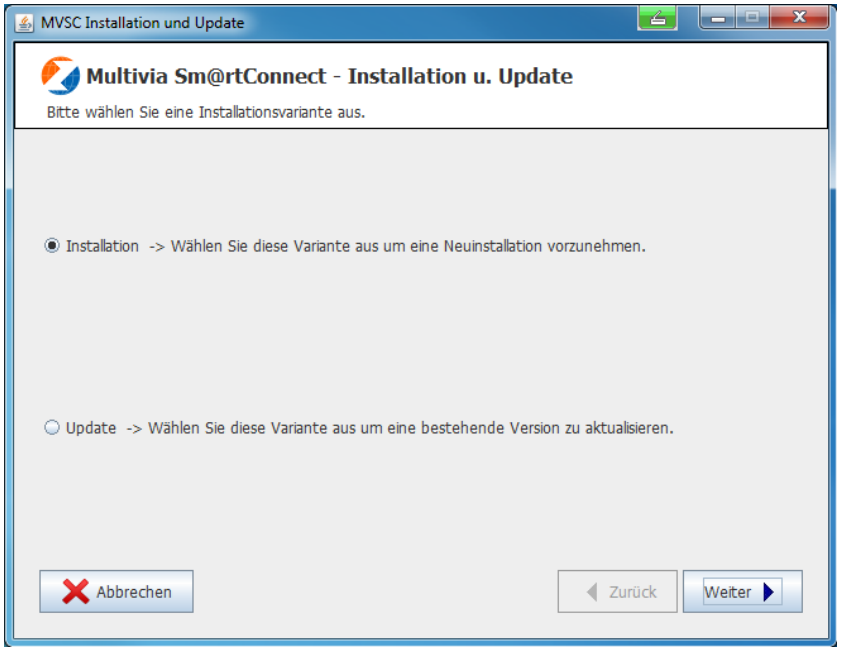
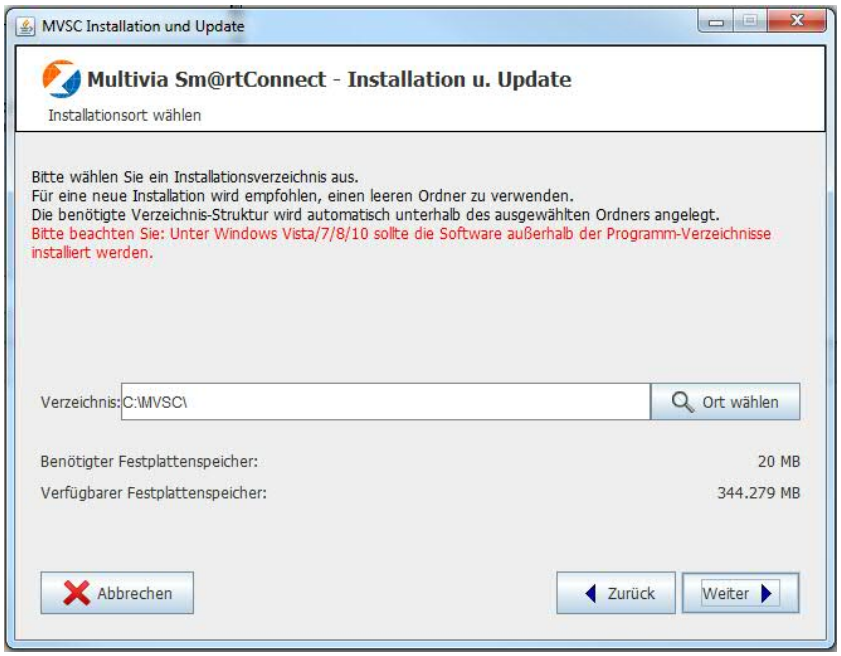
3. Installation

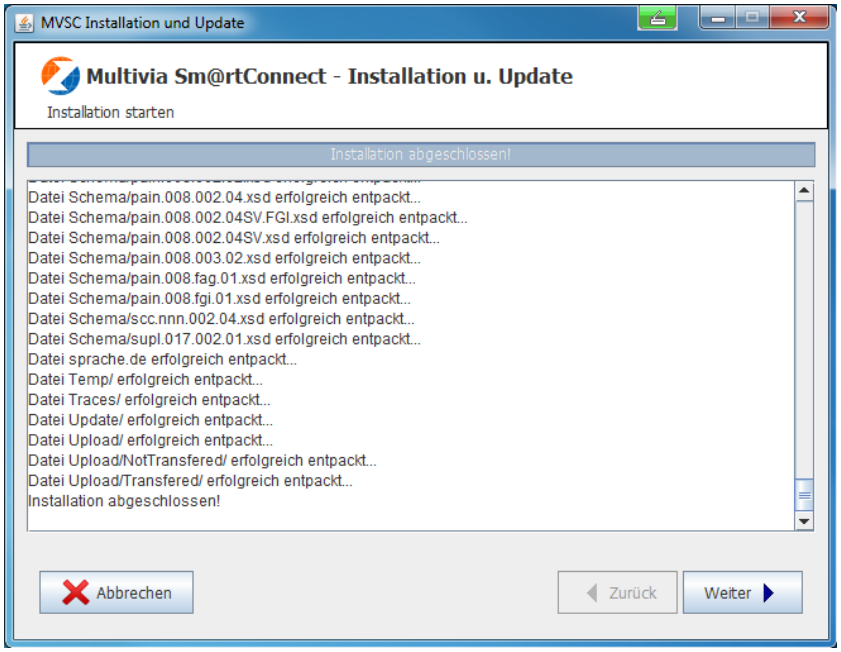
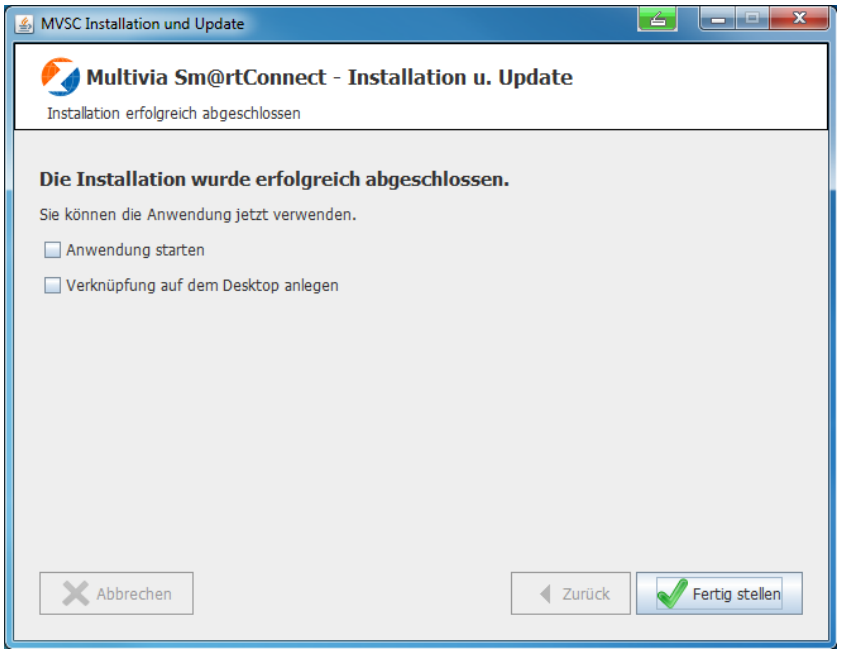
3.1. Installation mit Hilfe des Assistenten

Installation mit dem Assistenten "install.jar"

Seit der Programmversion 1.0 gibt es einen Installationsassistenten, der das Programm von einem Server herunterlädt und anschließend in wenigen Schritten durch die Installation führt. Dieser Installationsassistent "install.jar" ist in den folgenden Tabelle beschrieben:

Schritt	Vorgehen
1	Wählen Sie zunächst die Sprache aus, mit der Sie arbeiten möchten. Die ausgewählte Sprache wird für zukünftige Aufrufe des Programms dann als Defaultwert für Sie hinterlegt. Unabhängig davon können Sie die Sprache weiterhin wie in der Einleitung im Abschnitt "Mehrsprachigkeit" beschrieben umstellen. Für die Auswahl der Sprache wird Ihnen die folgende Maske angezeigt:  **Abb. 3.1. Sprachauswahl bei der Installation** Anschließend gehen Sie über die Schaltfläche "OK" zum nächsten Schritt über.
2	Starten Sie den Download des Programms und warten Sie ab, bis dieser durchgeführt wurde. Dabei wird Ihnen die folgende Maske angezeigt:  **Abb. 3.2. Download des Programms** Anschließend gehen Sie über die Schaltfläche "Weiter" zum nächsten Schritt über.
3	Wählen Sie aus, ob Sie eine Neuinstallation vornehmen möchten oder ob Sie Ihre bestehende Version aktualisieren möchten.

Schritt	Vorgehen
	Diese Auswahlmaske ist in der folgenden Abbildung dargestellt:  **Abb. 3.3. Installation oder Update einer bestehenden Version** Gehen Sie dann über die Schaltfläche "Weiter" zum nächsten Schritt über.
4	Wählen Sie ein Installationsverzeichnis aus. In der folgenden Abbildung ist die Maske "Installationsverzeichnis wählen" dargestellt:  **Abb. 3.4. Installationsverzeichnis wählen** Gehen Sie über die Schaltfläche "Weiter" zum nächsten Schritt über.
5	Warten Sie den Installationsvorgang ab. Dabei wird Ihnen die folgende Maske angezeigt:

Schritt	Vorgehen
	 **Abb. 3.5. Installationsvorgang** Anschließend gehen Sie über die Schaltfläche "Weiter" zum nächsten Schritt über.
6	Abschließend wird Ihnen die Bestätigung über den Abschluß der Installation angezeigt. Diese Bestätigungsmaske ist in der folgenden Abbildung dargestellt:  **Abb. 3.6. Installation abgeschlossen** Schließen Sie die Installation über die Schaltfläche "Fertig stellen" ab.

Update der Signaturversion einer Zugangs-ID

Ab der MVSC-Version 2.5.0 wird Ihnen, falls Sie eine Zugangs-ID mit einer kleineren Signaturversion als "A006" haben, eine Maske angezeigt, auf der Ihnen angeboten wird, ein Update auf die Signaturversion "A006" durchzuführen. Dabei werden Ihnen die Zugänge aufgelistet, die eine kleinere Signaturversion als "A006" haben.

Diese Maske ist in der folgenden Abbildung beispielhaft dargestellt:

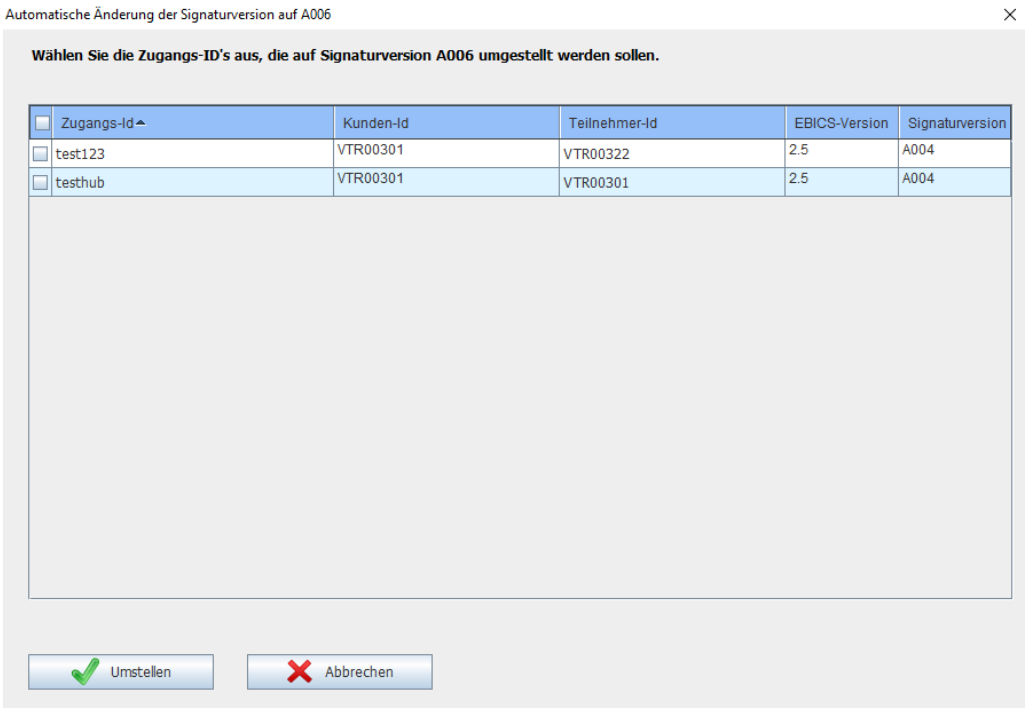


Abb. 3.7. Automatische Änderung der Signaturversion auf A006

Hier haben Sie die Möglichkeit, zunächst die Zugangs-IDs auszuwählen, für die Sie ein Update der Signaturversion auf "A006" durchführen möchten. Über die Schaltfläche "Umstellen" führen Sie das Update für die ausgewählten Zugangs-IDs durch.

Möchten Sie keinen der Zugänge umstellen, so wählen Sie die Schaltfläche "Abbrechen".

Update des Programms

Seit der MVSC-Version 1.0 verfügt das Programm über eine integrierte Update-Funktion. Nach der Anmeldung am Programm wird jeweils geprüft, ob neue Updates zur Verfügung stehen. Sollte ein Update verfügbar sein, erscheint eine entsprechende Meldung und die Durchführung des Updates kann bestätigt oder abgelehnt werden. Die Updateprüfung kann jederzeit über das Menü "Hilfe->Update" wiederholt werden.

4. Einrichtung

4.1. Programmstart

Legitimation

Die Anmeldung am Programm erfolgt mit einem MVSC-Administrator-Zugang. Das Startpasswort für den Administrator lautet "xxxx". Dieses muss bei der ersten Anmeldung geändert werden. Das neue Passwort muss aus mindestens acht Zeichen bestehen. Dabei muss es aus Buchstaben, Ziffern und mindestens einem Sonderzeichen bestehen.

Das Passwort kann danach jederzeit unter dem Reiter "Benutzer" geändert werden.

Des Weiteren kann der Administrator weitere Benutzer anlegen, die sich dann mit eigenen Passwörtern am Programm anmelden können.

4.2. Voraussetzungen für die EBICS-Kommunikation

Kunden-ID am EBICS-Bankrechner

Um am EBICS-Verfahren teilnehmen zu können, benötigt ein Kunde eine Kunden-ID, die auf dem EBICS-Bankrechnersystem eingerichtet sein muss. Zu einer Kunden-ID können verschiedene Teilnehmer-IDs eingerichtet werden, die in der Regel die Mitarbeiter eines Unternehmens wiederspiegeln. Die Berechtigungen eines jeden Mitarbeiters sind im EBICS-Bankrechner an der jeweiligen Teilnehmer-ID hinterlegt und können nur dort geändert werden.

BPD-Blatt

Zu jeder Teilnehmer-ID existiert ein "BPD-Blatt", das unter anderem auch die vollständigen Informationen zu dessen Berechtigungen beinhaltet. Dazu gehören die Verbindungsdaten des EBICS-Servers (Hostname/ URL), die zugelassenen Auftragsarten, die bei der Initialisierung abzugleichenden öffentlichen Bankschlüssel (Hashwerte) sowie eine Auflistung der Konten, für die eine Teilnehmer-ID berechtigt wurde. Um unter dem Reiter "Zugänge" eine Zugangs-ID einzurichten, müssen die Informationen "Kunden-ID", "Teilnehmer-ID", "Hostname" und "URL-Adresse" in die Maske übertragen und dann gespeichert werden.

4.3. Internetverbindung erfassen

Internetverbindung

Für die EBICS-Kommunikation ist eine Internetverbindung erforderlich. Die Internetverbindung wird unter dem Reiter "Internet" für alle Anwender und alle EBICS-Zugänge zentral hinterlegt.

Nutzung ohne Proxy-Server

Wenn die Verbindung zum Internet nicht über einen Proxy-Server hergestellt werden soll, müssen in der Maske "Internetverbindung verwalten" keine Anpassungen vorgenommen werden.

Die Maske "Internetverbindung verwalten" ist in der folgenden Abbildung dargestellt:

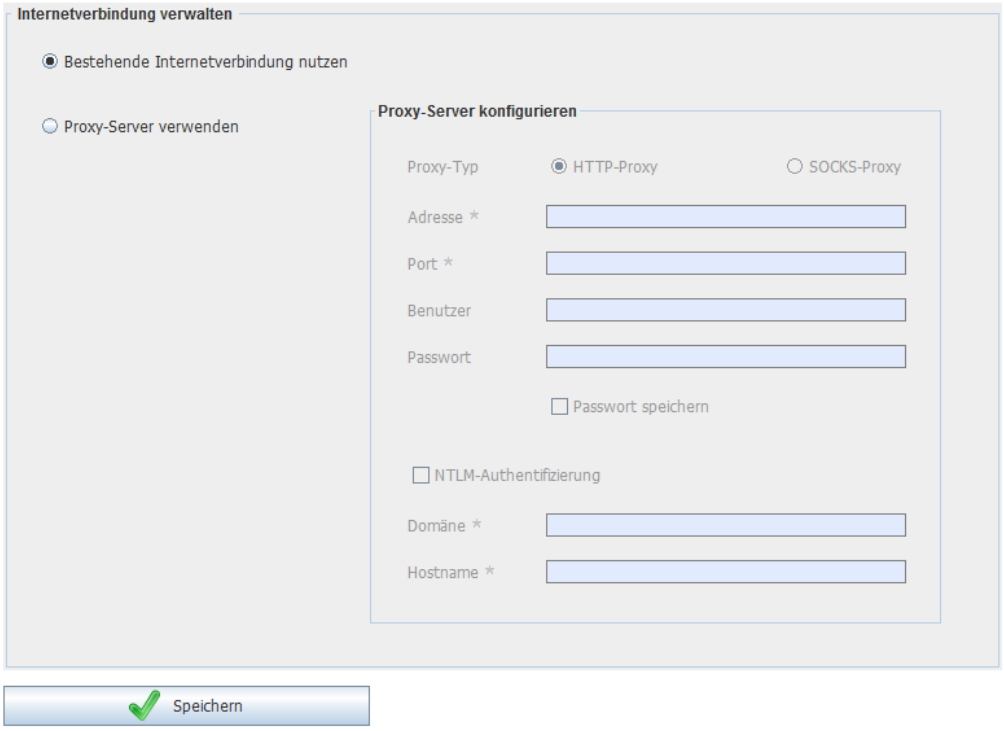


Abb. 4.1. Internet-Nutzung ohne Proxy

Nutzung eines Proxy-Servers

Sollte ein Proxy-Server zum Verbindungsaufbau mit dem Internet benötigt werden, so müssen mindestens Adresse (oder IP) und Port des Servers in die dafür vorgesehenen Felder eingegeben werden. Da einige Proxy-Server eine Authentifizierung verlangen, können Benutzername und Passwort ebenfalls im Programm hinterlegt werden.

Passwort für den Proxy-Server

Falls das Passwort für den Proxy-Server nicht im Programm gespeichert werden soll, kann die Eingabe unter Verwendung der Benutzeroberfläche auch während einer Datenübertragung erfolgen. Im Konsolenmodus muss das Passwort für den Proxy-Server dagegen, falls es benötigt wird, auch hinterlegt werden.

Nutzung der NTLM-Authentifizierung

"NTLM" ist ein von Microsoft entwickeltes Authentifizierungsverfahren für Rechnernetze, das die Authentifizierung innerhalb einer Domäne über den Namen der jeweiligen Arbeitsstation sicherstellt. Um diese Art der Authentifizierung zu nutzen, müssen die Domäne, in der sich der angesteuerte Proxy-Server befindet, sowie der Name der eigenen Arbeitsstation (Hostname) angegeben werden.

Anmerkung
Die NTLM-Authentifizierung kann nur in entsprechend eingerichteten Netzwerken verwendet werden. In den meisten Netzwerken ist die direkte Authentifizierung über einen angegebenen Proxy-Server ausreichend.

4.4. EBICS-Zugangsdaten erfassen

Menüpunkt

Die EBICS-Zugangsdaten werden unter dem Reiter "Zugänge" erfasst. Die Einrichtung eines funktionstüchtigen EBICS-Zugangs beinhaltet in MVSC mehrere Schritte:

Schritt	Vorgehen
1	Übertragen Sie die EBICS-Zugangsdaten vom BPD-Blatt in die Eingabemaske und speichern Sie Ihre Eingaben über die Schaltfläche "Speichern" ab.
2	Legen Sie über die Schaltfläche "Neu generieren" ein neues Sicherheitsmedium an oder ordnen Sie ein vorhandenes Sicherheitsmedium zu.
3	Initialisieren Sie das angegebene Sicherheitsmedium am EBICS-Bankrechner (Bekanntgabe der eigenen öffentlichen Schlüssel). **Achtung** Als Ergebnis dieses Schritts erhalten Sie einen sogenannten "Initialisierungsbrief". Reichen Sie den Initialisierungsbrief schriftlich bei Ihrer Bank ein, damit die Bank Ihre Schlüssel freischalten kann. Erst wenn die Freischaltung erfolgt ist, kann mit dem nächsten Schritt fortgefahren werden.
4	Rufen Sie Ihre Berechtigungen ab. **Anmerkung** Im Rahmen dieses Vorgangs werden gegebenenfalls das Serverzertifikat und die öffentlichen Schlüssel der Bank abgeholt.

Über den Menüpunkt "Konfiguration -> Zugangs-ID einrichten" können Sie einen Assistenten starten, der Sie bei der Anlage einer Zugangs-ID unterstützt. Dabei werden die nachfolgenden Informationen Schritt für Schritt abgefragt.

Kartenleser auswählen

Falls Sie für Ihren EBICS-Zugang eine Chipkarte als Signaturmedium verwenden möchten, ist es notwendig, einen Standard-Chipkartenleser festzulegen. Sie können den Standard-Chipkartenleser jederzeit über das Menü "Konfiguration -> Kartenleser auswählen" ändern. Der aus der Liste ausgewählte Standard-Chipkartenleser wird für alle zukünftigen Zugriffe auf die Chipkarte verwendet.

Wurde noch kein Standard-Chipkartenleser festgelegt oder der festgelegte Standard-Chipkartenleser nicht gefunden, so bietet MVSC Ihnen eine Auswahlliste an.

Die Auswahlliste ist in der folgenden Abbildung dargestellt:

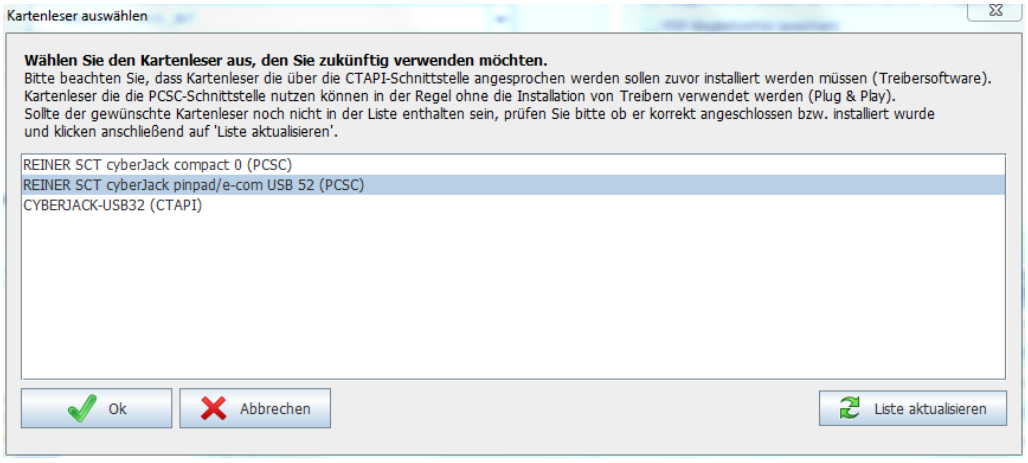


Abb. 4.2. Standard-Chipkartenleser festlegen

Identifizierung der Zugangsdaten

Die eingegebenen Zugangsdaten werden bei der weiteren Nutzung des Programms immer wieder über die eingegebene Zugangs-ID identifiziert.

Achtung
Die Zugangs-ID selber kann im Nachhinein nicht mehr verändert werden.

Anlagevorgang

In der folgenden Tabelle wird die Anlage einer neuen Zugangs-ID erläutert. Dabei wird im zweiten Schritt zwischen den drei Signaturmedien

- Zertifikat
- Sicherheitsdatei
- Chipkarte

unterschieden. Diese drei Alternativen werden in den Schritten 2a, 2b und 2c beschrieben. Es ist also jeweils nur einer der drei Schritte 2a, 2b oder 2c durchzuführen.

Tipp
Es wird empfohlen, das Zertifikat zu nutzen.

Achtung
Ab der EBICS-Version "EBICS 3.0" können keine neuen Chipkarten und Sicherheitsdateien mehr generiert oder initialisiert werden. Bestehende Chipkarten oder Sicherheitsdateien können aber weiterhin verwendet werden.

Schritt	Vorgehen
1	Übertragen Sie Ihre EBICS-Zugangsdaten vom BPD-Blatt in die Erfassungsmaske des Reiters "Zugänge". Dabei ist der Begriff für die Zugangs-ID grundsätzlich frei wählbar. Die Länge darf dabei aber nur maximal 30 Zeichen betragen und es dürfen nur die folgenden Zeichen verwendet werden: • Groß- und Kleinbuchstaben (A - Z, a - z) • Umlaute (Ä, ä, Ü, ü, Ö, ö) • Ziffern (0 - 9) • Unterstrich **Anmerkung** Altzugänge sind von dieser Einschränkung unberührt. In der folgenden Abbildung ist die Erfassungsmaske dargestellt:

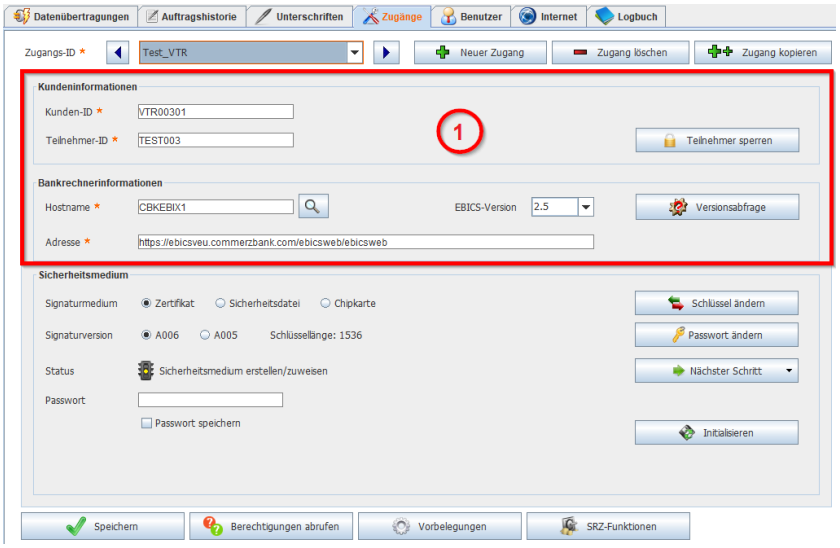
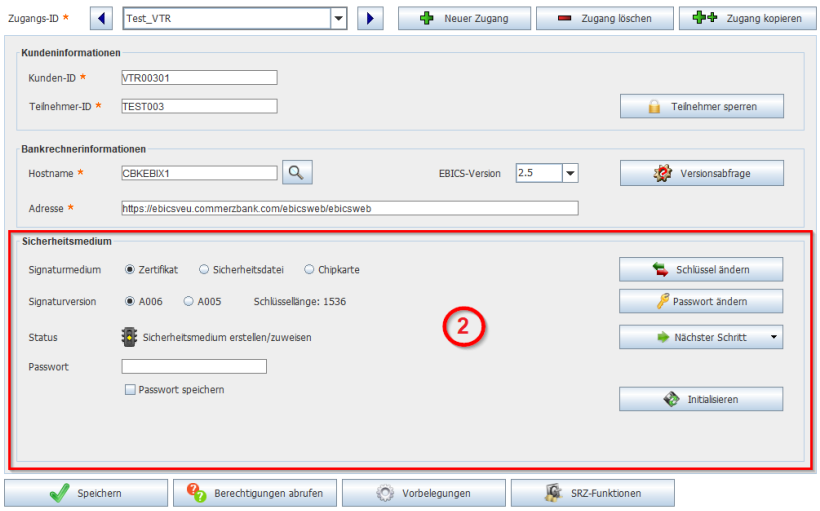
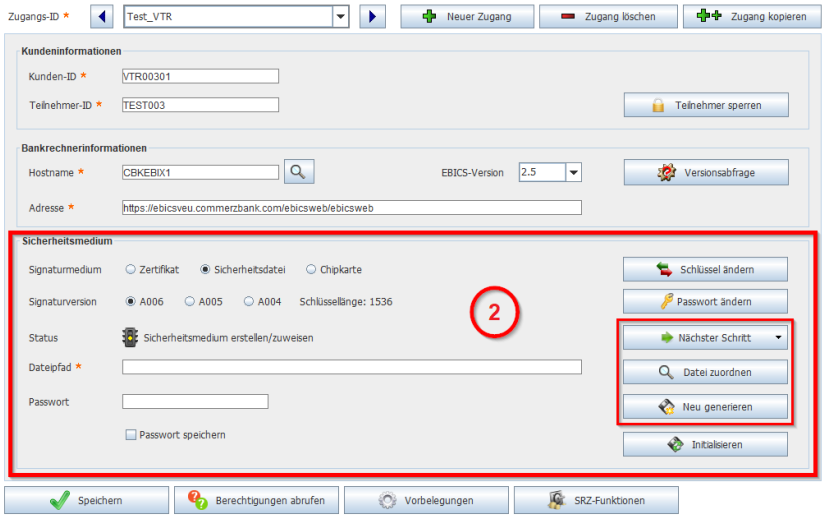


Abb. 4.3. Datenerfassung in Multivia Sm@rtConnect, Schritt 1

Erfassen Sie zunächst die auf dem BPD-Blatt angegebenen Daten unter Angabe einer beliebigen Zugangs-ID im oberen Bereich der Maske. Die folgenden Felder sind dabei zu füllen:

Schritt	Vorgehen
	<table><tr><th>Bezeichnung MVSC</th><th>Bezeichnung BPD-Blatt</th></tr><tr><td>Kunden-ID</td><td>Kunden-ID (Seite 1)</td></tr><tr><td>Teilnehmer-ID</td><td>Teilnehmer-ID (Seite 2)</td></tr><tr><td>Hostname</td><td>EBICS-Bankname (Seite 1)</td></tr><tr><td>Adresse</td><td>Bankparameter-URL/ EBICS-URL (Seite 1)</td></tr></table> Wählen Sie den Hostnamen und die EBICS-Version aus und speichern Sie anschließend Ihre eingegebenen Daten über die Schaltfläche "Speichern" ab. Je nach Signaturmedium fahren Sie dann mit Schritt 2a, 2b oder 2c fort: • Schritt 2a: Zertifikat • Schritt 2b: Sicherheitsdatei • Schritt 2c: Chipkarte
2a	Nachdem die Daten aus Schritt 1 gespeichert wurden, ist das Sicherheitsmedium zu konfigurieren. In diesem Beispiel soll ein Zertifikat genutzt werden. **Signaturmedium Zertifikat:** In der folgenden Abbildung ist die Erfassungsmaske des Reiters "Zugänge" zur Konfiguration des Sicherheitsmediums am Beispiel des Zertifikats dargestellt:  **Abb. 4.4. Datenerfassung in Multivia Sm@rtConnect, Schritt 2a** **Voraussetzungen für die Nutzung eines Zertifikats:** • Deutschland: Es wird mindestens die EBICS-Version 2.5 eingesetzt. • Europa außer Deutschland: Es wird mindestens die EBICS-Version 3.0 eingesetzt. **Vorgehensweise zur Nutzung eines Zertifikats:** • Wählen Sie als Signaturmedium "Zertifikat" aus. • Wählen Sie aus, welcher Signaturversion Ihr Zertifikat entspricht (A006/ A005). • Vergeben Sie gemäß der angezeigten Passwortregeln ein Passwort für Ihre Zertifikat. • Wiederholen Sie das zuvor angegebene Passwort. • Optional: Hinterlegen Sie Ihr Passwort für das Zertifikat (Kontrollkästchen "Passwort speichern").
2b	Nachdem die Daten aus Schritt 1 gespeichert wurden, ist das Sicherheitsmedium zu konfigurieren. In diesem Beispiel soll eine Sicherheitsdatei genutzt werden. **Signaturmedium Sicherheitsdatei:** In der folgenden Abbildung ist die Erfassungsmaske des Reiters "Zugänge" zur Konfiguration des Sicherheitsmediums am Beispiel der Sicherheitsdatei dargestellt:

Schritt	Vorgehen
	 **Abb. 4.5. Datenerfassung in Multivia Sm@rtConnect, Schritt 2b** **Vorgehensweise zur Nutzung einer bestehenden Sicherheitsdatei:** • Geben Sie an, welcher Signaturversion die Schlüssel in der Zieldatei entsprechen (A006/ A005/ A004). • Betätigen Sie die Schaltfläche "Datei zuordnen". • Wählen Sie die bereits bestehende Sicherheitdatei aus und bestätigen Sie den Auswahldialog. • Speichern Sie Ihre Zugangsdaten über die Schaltfläche "Zugang speichern". **Vorgehensweise zur Generierung einer neuen Sicherheitsdatei (ab EBICS 3.0 nicht mehr möglich):** • Geben Sie an, welche Signaturversion bei der Generierung der Sicherheitsdatei erzeugt werden soll (A006/ A005/ A004). • Betätigen Sie die Schaltfläche "Neu generieren". • Geben Sie einen Pfad bzw. Dateinamen an, unter dem die Sicherheitsdatei abgelegt werden soll. • Vergeben Sie gemäß der angezeigten Passwortregeln ein Passwort für Ihre neue Sicherheitsdatei. • Wiederholen Sie das zuvor angegebene Passwort. • Optional: Hinterlegen Sie Ihr Passwort für die soeben generierte Sicherheitsdatei (Kontrollkästchen "Passwort speichern").
2c	Nachdem die Daten aus Schritt 1 gespeichert wurden, ist das Sicherheitsmedium zu konfigurieren. In diesem Beispiel soll eine Chipkarte genutzt werden. **Signaturmedium Chipkarte:** In der folgenden Abbildung ist die Erfassungsmaske des Reiters "Zugänge" zur Konfiguration des Sicherheitsmediums am Beispiel der Chipkarte dargestellt:

Schritt	Vorgehen

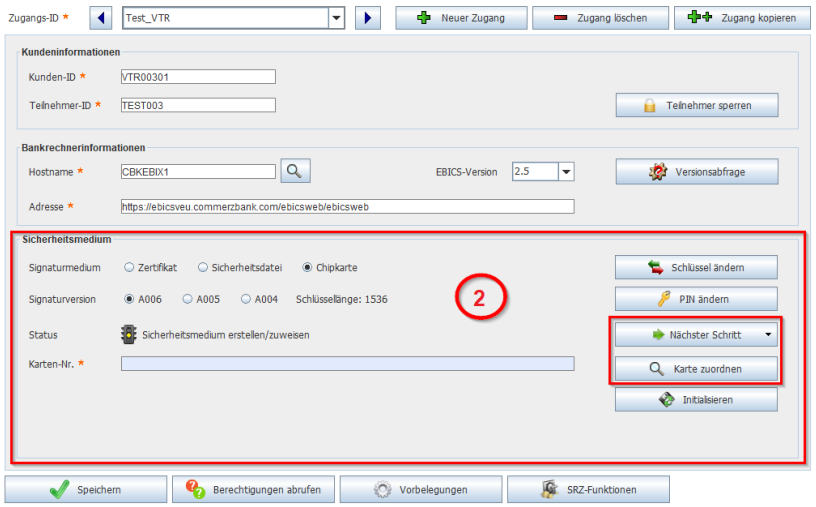


Abb. 4.6. Datenerfassung in Multivia Sm@rtConnect, Schritt 2c

Voraussetzungen für die Nutzung einer Chipkarte:

- Ein Chipkartenleser ist am Computer installiert und angeschlossen.
- Der Standard-Chipkartenleser wurde festgelegt.
- Es wird eine EBICS-fähige Chipkarte (z.B. eine Karte vom Typ "SECCOS 6") verwendet.
- Die initialen PINs sind bekannt bzw. wurden bereits geändert.

Vorgehensweise zur Zuordnung einer neuen Chipkarte (ab EBICS 3.0 nicht mehr möglich):

- Wählen Sie als Signaturmedium die "Chipkarte" aus.
- Wählen Sie aus, welcher Signaturversion die Schlüssel auf Ihrer Chipkarte entsprechen (A006/ A005/ A004).
- Betätigen Sie die Schaltfläche "Karte zuordnen"

3

Nun sind alle Daten für den EBICS-Zugang erfasst und das Sicherheitsmedium kann am Bankrechnersystem initialisiert werden.

Die Vorgehensweise ist in der folgenden Abbildung dargestellt:

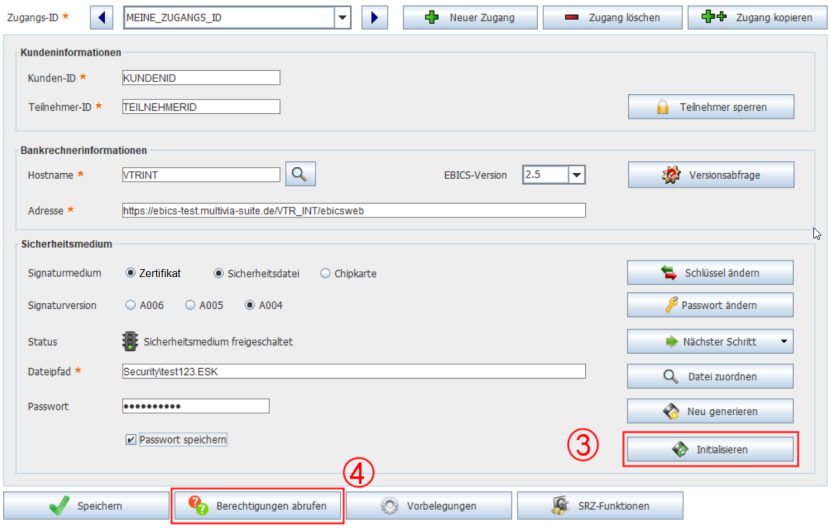
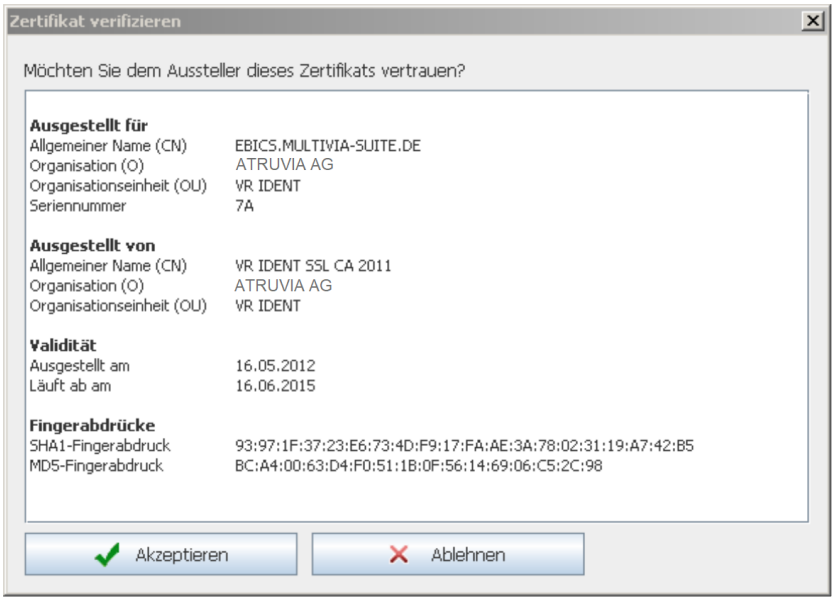
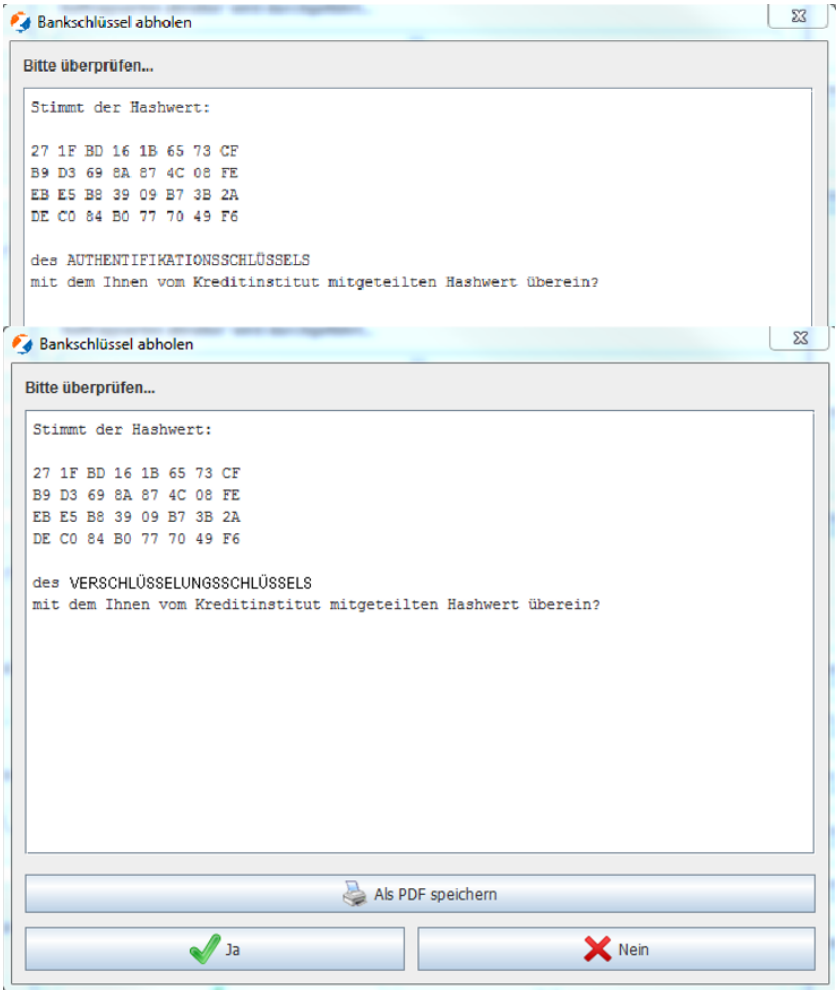
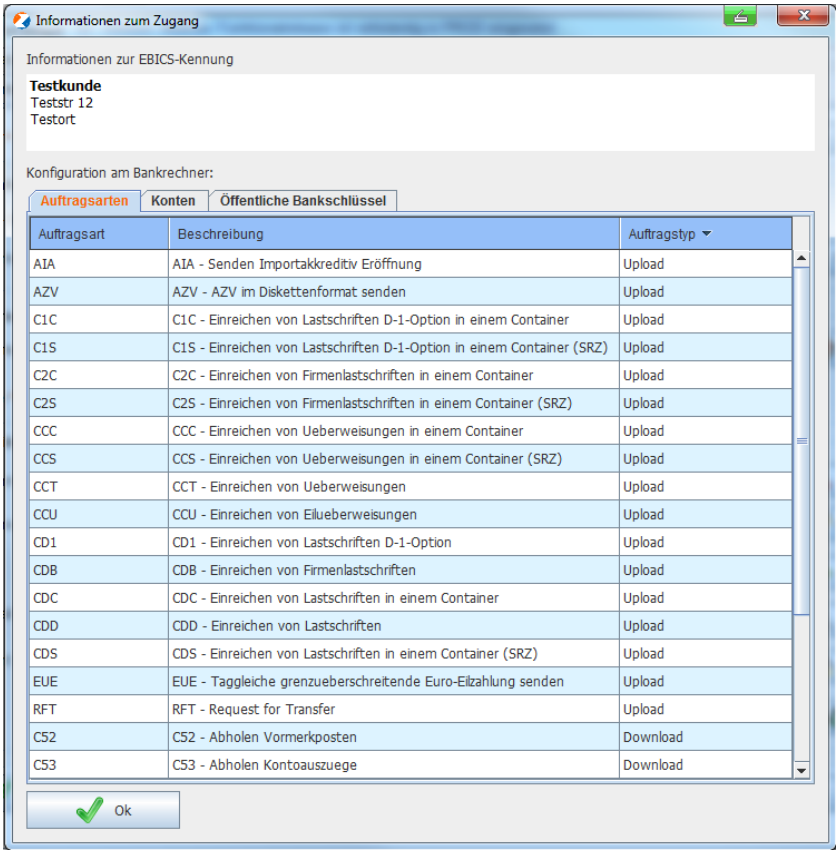


Abb. 4.7. Datenerfassung in Multivia Sm@rtConnect, Schritt 3

Vorgehensweise zur Initialisierung des Sicherheitsmediums:

Schritt	Vorgehen
	Betätigen Sie zunächst die Schaltfläche "Initialisieren". Bei diesem Vorgang werden die öffentlichen Schlüssel Ihres Sicherheitsmediums zum EBICS-Bankrechner übertragen und den dort hinterlegten Zugangsdaten (Teilnehmer-ID) zugeordnet. Als "Quittung" erhalten Sie einen sogenannten Initialisierungsbrief, der im Installationsverzeichnis unter "Download/ Dokumente" als PDF-Datei abgelegt wird. Durch Unterschrift auf dem INI-Brief bestätigen Sie Ihr eigenes Signaturmedium. Der INI-Brief ist auf einem unabhängigen Transportweg (z.B. per Fax) an den Betreiber des EBICS-Bankrechners zu übermitteln. Mit Hilfe der darauf abgedruckten Hashwerte kann die Teilnehmer-ID am Bankrechnersystem freigeschaltet werden. Ist dies geschehen, so ist der EBICS-Zugang (bzw. die Zugangs-ID in MVSC) vollständig initialisiert und funktionstüchtig. **Anmerkung** Unter Umständen ist MVSC das SSL-Zertifikat (für die https-Verbindung) des jeweiligen EBICS-Bankrechners noch nicht bekannt. In diesem Fall holt das Programm das Zertifikat des Servers ab und zeigt Informationen über den Aussteller des Zertifikats an. Ist der Aussteller vertrauenswürdig, kann das Zertifikat akzeptiert werden, andernfalls sollte es abgelehnt werden. Ohne ein akzeptiertes SSL-Zertifikat kann keine EBICS-Kommunikation zustande kommen. **Anmerkung** Es ist möglich, dass ein Zertifikat nicht importiert werden kann, weil es nicht von einem offiziellen Trustcenter (z.B. "Verisign") ausgestellt wurde. Sollte dies der Fall sein, kann nicht mit dem entsprechenden Bankrechnersystem kommuniziert werden. Anschließend kann der Initialisierungsvorgang in MVSC endgültig abgeschlossen werden.
4	Für die EBICS-Kommunikation über das HTTPS-Protokoll werden entsprechende SSL-Zertifikate benötigt. Sollte das Zertifikat noch nicht vorhanden sein, wird es in diesem Schritt abgeholt. Häufig sind die benötigten Zertifikate aber bereits im System hinterlegt,- deshalb ist dieser Schritt nicht immer erforderlich. Wurde das Zertifikat abgeholt, so werden Ihnen die Informationen zur Kontrolle des Zertifikats angezeigt. Diese Anzeige ist in der folgenden Abbildung beispielhaft dargestellt:  **Abb. 4.8. Verifizierung des Zertifikats**

Schritt	Vorgehen
	Achtung In den angezeigten Informationen muss erkennbar sein, dass das Zertifikat von dem in den Zugangsdaten konfigurierten Server stammt. Zum Beispiel sollte der Wert "Ausgestellt für" einen Teil der vom BPD-Blatt übernommenen EBICS-Adresse/ URL enthalten.
5	Um die für die Zugangs-ID zugelassenen Auftragsarten ausführen zu können, müssen diese zuerst vom Bankrechnersystem abgeholt und von MVSC gespeichert werden. Betätigen Sie dafür die Schaltfläche "Berechtigungen abrufen". Sollte dies Ihre erste Transaktion mit dem jeweiligen Bankrechner sein, holt MVSC während dieses Vorgangs automatisch die öffentlichen Schlüssel des Bankrechnersystems ab. Bei der Bestätigung der öffentlichen Schlüssel ist folgendes zu beachten: • Die Schlüssel werden in aufbereiteter Form angezeigt und müssen durch Sie verifiziert werden. Diese Anzeige ist in der folgenden Abbildung dargestellt:  **Abb. 4.9. Abholen des Bankschlüssels** • Vergleichen Sie die angezeigten Hashwerte mit denen, die auf Ihrem BPD-Blatt auf Seite 2 abgedruckt sind. • Stimmen die Werte überein, bestätigen Sie beide Schlüssel mit Hilfe der dafür vorgesehenen Schaltfläche "Ja". Stimmen die Werte jedoch nicht überein, so dürfen diese aus Sicherheitsgründen nicht bestätigt und nicht gespeichert werden (Manipulationsverdacht). Wurden die öffentlichen Schlüssel bestätigt, wird automatisch mit dem Abholen der Berechtigungen fortgefahren.

Schritt	Vorgehen
6	Wenn die Berechtigungen erfolgreich abgeholt wurden, ist auch die Liste der ausführbaren Auftragsarten mit dem EBICS-Bankrechner synchronisiert worden. Falls zum Beispiel am EBICS-Bankrechner eine Auftragsart neu zugeordnet wurde, kann diese nach der Synchronisierung der Berechtigungen in MVSC ausgeführt werden. Außerdem können die Konten eingesehen werden, für die der jeweilige Zugang berechtigt ist, Zahlungsverkehrsdateien einzureichen. Die Maske ist in der folgenden Abbildung dargestellt:  **Abb. 4.10. Informationen zum Zugang** Nachdem die Liste der Auftragsarten erstmalig synchronisiert wurde, kann die Schaltfläche "Vorbelegungen" betätigt werden. Im folgenden Dialog können die unter dem Reiter "Datenübertragung" vorbelegten Verzeichnispfade eingestellt werden. Auch die Nachverarbeitung von gesendeten Dateien kann hier angepasst werden. Nähere Informationen dazu finden Sie im Kapitel "Vorbelegungen".

Schlüssel ändern

Um Ihre Teilnehmerschlüssel am Bankrechner zu ändern, steht Ihnen die Funktion "Schlüssel ändern" zur Verfügung.

Der Aufruf dafür ist in der folgenden Abbildung dargestellt:

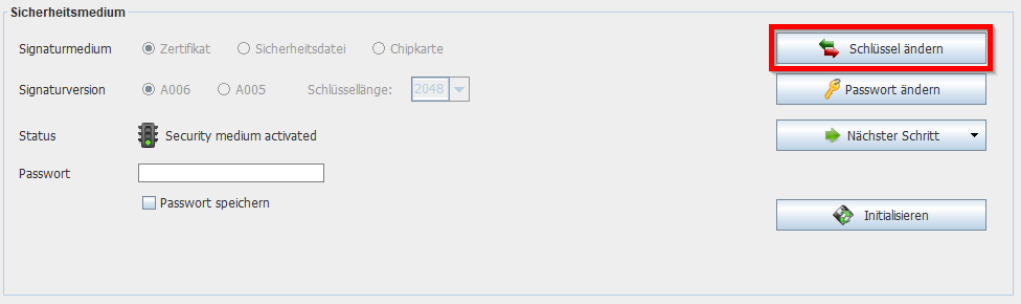


Abb. 4.11. Aufruf der Schlüsseländerung

Wählen Sie im folgenden Dialog Ihr Signaturmedium, Ihre Signaturversion und die Schlüssellänge aus.

Dies ist in den folgenden drei Abbildungen beispielhaft dargestellt:

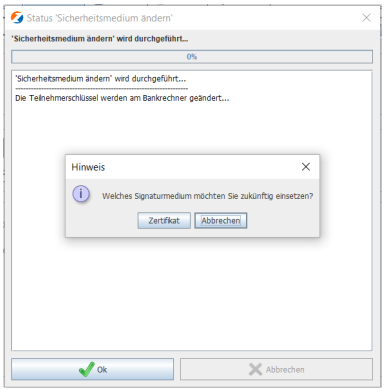


Abb. 4.12. Schlüsseländerung - Auswahl des Signaturmediums

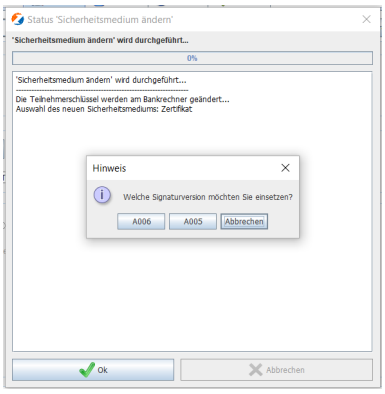


Abb. 4.13. Schlüsseländerung - Auswahl der Signaturversion

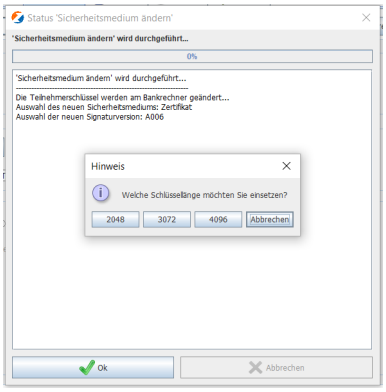


Abb. 4.14. Schlüsseländerung - Auswahl der Schlüssellänge

4.5. Zugangsdaten importieren

Import aus bestehender Installation

Sollte bereits eine MVSC-Version installiert sein, können die dort hinterlegten Konfigurationsdaten importiert werden. Voraussetzung für einen erfolgreichen Datenimport ist die Angabe des Quell-Installationsverzeichnisses. Außerdem muss vor dem Start des Importvorgangs das Administrator-Passwort der Quellinstallation eingegeben werden. Der Datenimport kann über den Menüpunkt "Datei->Import" gestartet werden.

Anmerkung
Wenn die Benutzer der Anwendung aus der Quellinstallation übernommen werden, wird auch das Passwort des Administrators in die Zielinstallation übernommen.

Importvorgang

Um Daten aus einer anderen MVSC-Installation zu importieren, gehen Sie wie folgt vor:

Schritt	Vorgehen
1	Geben Sie das Verzeichnis der Quellinstallation ein. In diesem Verzeichnis sollten sich z.B. die Dateien "MVSC.jar" und "defaults.xml" befinden.
2	Wählen Sie aus, welche Daten aus der Quellinstallation importiert werden sollen: • Zugangs-IDs (Alle EBICS-Konfigurationsdaten aus der Erfassungsmaske des Reiters "Zugänge" werden in die Zielinstallation übernommen.) • Benutzer (Alle Benutzer werden einschließlich ihrer Passwörter in die Zielinstallation übernommen. Auch das Administratorpasswort wird übernommen.) • Interneteinstellungen (Die unter dem Reiter "Internet" hinterlegten Internet-Verbindungsdaten werden in die Zielinstallation übernommen und dort ggf. überschrieben.)
3	Starten Sie den Import-Vorgang über die Schaltfläche "Importieren".
4	Geben Sie das Administratorpasswort der Quellinstallation ein.
5	Kontrollieren Sie die importierten Daten. **Anmerkung** Beim Import von Zugangs-IDs werden unter Umständen die unter "Vorbelegungen" eingestellten Verzeichnispfade an die Zielinstallation angepasst. Diese sind nach Abschluss des Importvorgangs zu überprüfen und ggf. zu korrigieren. **Anmerkung** Sollte eine zu importierende Zugangs-ID bereits in der Zielinstallation existieren, so muss für diese EBICS-Konfiguration eine neue Bezeichnung (Zugangs-ID) vergeben werden.

In der folgenden Abbildung ist die Maske zum Datei-Import dargestellt:

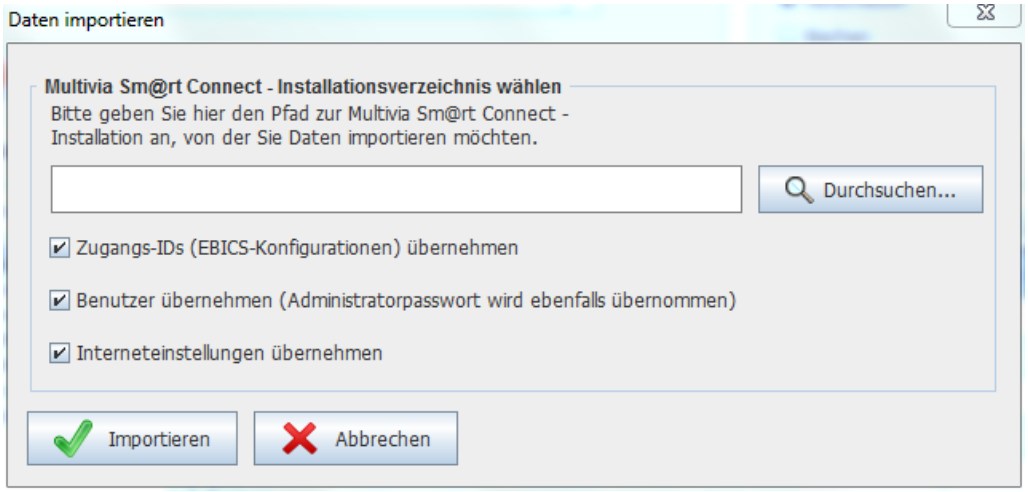


Abb. 4.15. Datei-Import von Bestandsdaten bei Neuinstallation von MVSC

Kontrolle

Nach Abschluss der Import-Aktivitäten können Sie im sogenannten "Import-Protokoll" nachlesen, welche Daten importiert wurden und ob währenddessen Fehler aufgetreten sind. Außerdem ist es empfehlenswert, folgendes zu prüfen:

- Sind die Pfadeinstellungen unter "Vorbelegungen" noch korrekt?
- Müssen Passwörter für Sicherheitsdateien erneut hinterlegt werden? (Konsolenaufruf)
- Werden noch Dokumente aus der Altinstallation benötigt? (z.B. INI-Briefe)

4.6. Lizenzserver

Lizenzschlüssel-verwaltung

Jedes MVSC-Softwarepaket muss durch einen Lizenzschlüssel am Lizenzserver registriert sein. Die Prüfung der Gültigkeit des Lizenzschlüssels erfolgt beim Login des Programms "MVSC". An dieser Stelle wird geprüft, ob das Programm bereits registriert ist. Bei nicht ordnungsgemäßer Registrierung erscheint beim Login ins Programm eine Meldung, wie lange das Programm noch ohne Registrierung lauffähig ist. Generell kann das Programm ohne Registrierung 60 Tage uneingeschränkt genutzt werden. Danach ist "MVSC" nur noch eingeschränkt nutzbar. Dateiübertragungen sind dann nicht mehr möglich.

Die Anmeldemaske ohne Registrierung ist in der folgenden Abbildung dargestellt:

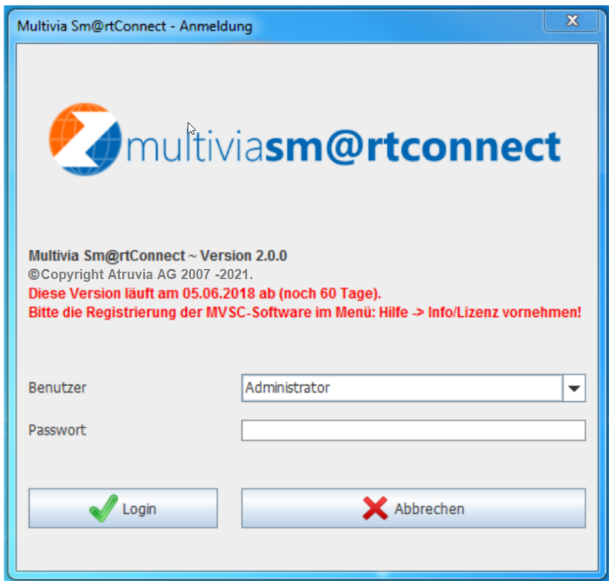


Abb. 4.16. Login ohne ordnungsgemäße Registrierung

Die Anmeldemaske mit erfolgter Registrierung ist in der folgenden Abbildung dargestellt:

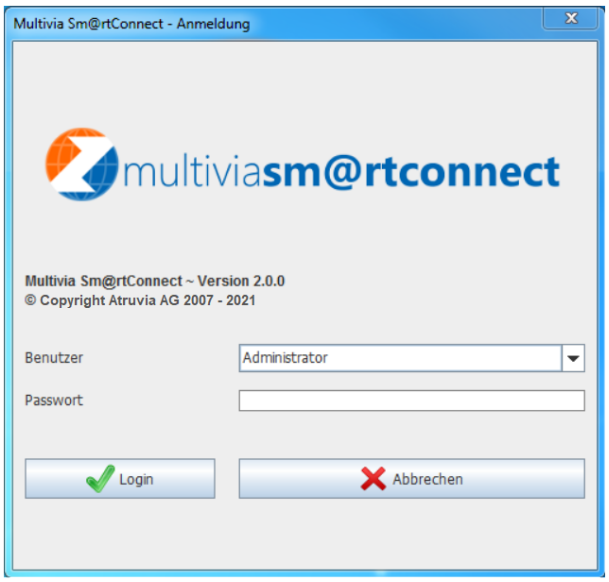


Abb. 4.17. Login mit ordnungsgemäßer Registrierung

Lizenzschlüssel-registrierung

Die Registrierung am Lizenzserver erfolgt im Programm MVSC über den Menüpunkt "Info/ Lizenz" im Menü "Hilfe".

Das Menü "Hilfe" ist in der folgenden Abbildung dargestellt:

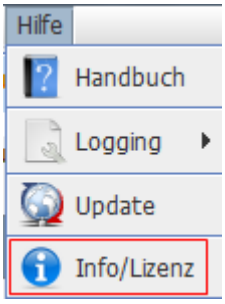


Abb. 4.18. Info/ Lizenz

Nach Eingabe des Lizenzschlüssels kann das Programm "MVSC" sofort über die Schaltfläche "Registrieren & Prüfen" aktiviert und freigeschaltet werden. Bei erfolgreicher Registrierung wird eine Bestätigungsmeldung angezeigt. Der Anwender kann jederzeit den Status des Lizenzschlüssels überprüfen.

In der folgenden Abbildung ist die Maske zur Eingabe des Lizenzschlüssels dargestellt:

Abb. 4.19. Lizenzschlüssel registrieren und prüfen

In der folgenden Abbildung ist die Bestätigungsmeldung der Registrierung dargestellt:

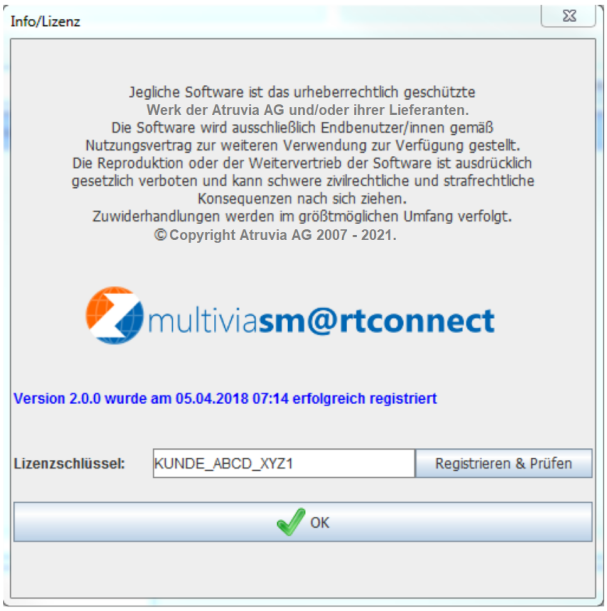


Abb. 4.20. Lizenzschlüssel erfolgreich registriert

5. Nutzung von MVSC

5.1. Allgemeines

Nutzungsmöglichkeiten

Um die Voraussetzungen für die Nutzung von MVSC zu schaffen, sollte zunächst die Einrichtung der verschiedenen Zugänge (Internet/ EBICS) durchgeführt werden. Ist dies geschehen, so können direkt über die Oberfläche Daten übertragen werden. Für die Nutzung ohne Benutzeroberfläche sind dagegen noch weitere Voraussetzungen zu beachten.

5.2. Datenübertragung im Dialog

5.2.1. Dateien senden

Upload-Auftragsart ausführen

Um mit Hilfe von MVSC Dateien per EBICS übertragen zu können, wechseln Sie auf den Reiter "Datenübertragungen". Von dort aus können Sie in wenigen Schritten eine Datenübertragung starten, vorausgesetzt die Konfigurationseinstellungen wurden korrekt vorgenommen.

In der folgenden Abbildung ist beispielhaft die Maske zur Durchführung einer Datenübertragung (Datei-Upload) dargestellt:

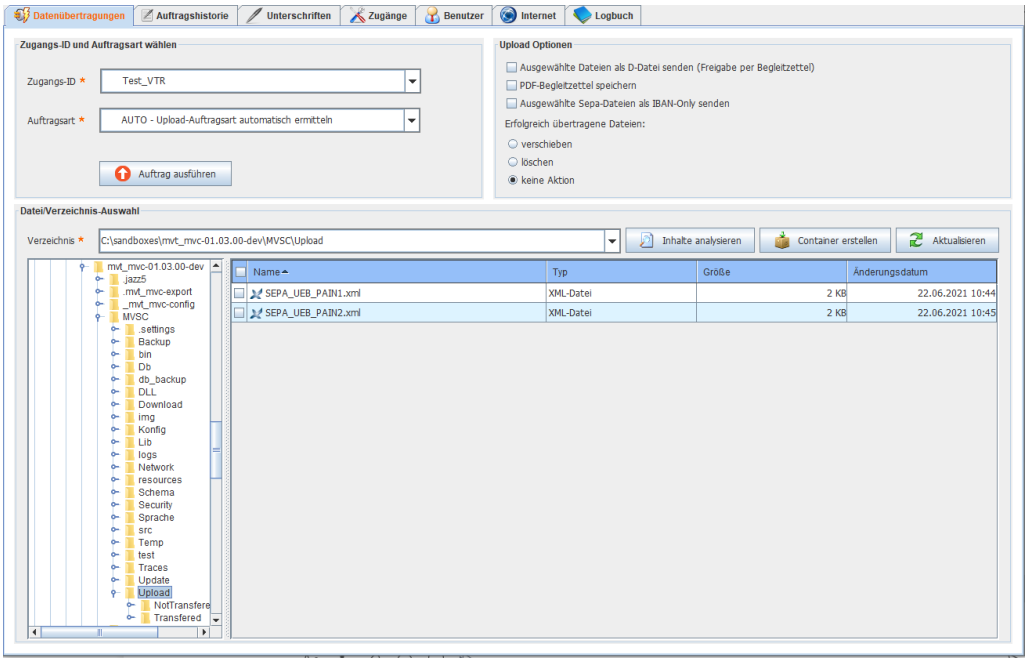


Abb. 5.1. Datei-Upload

Zur Durchführung der Dateiübertragung gehen Sie wie folgt vor:

1. Wählen Sie die Zugangs-ID (EBICS-Konfiguration) aus, mit der die Daten übertragen werden sollen.
2. Geben Sie an, mit welcher Auftragsart die Datei(en) gesendet werden soll(en).
3. Selektieren Sie die zu übertragenden Dateien über die dafür vorgesehenen Kontrollkästchen innerhalb der Tabelle.
4. Betätigen Sie die Schaltfläche "Auftrag ausführen", um die ausgewählten Dateien zu übertragen.

Tipp
Bei Auswahl der Auftragsart "AUTO" werden alle Uploaddateien aus dem Uploadverzeichnis mit der ermittelten Auftragsart zum Bankrechner übertragen.

Auftragsarten und Dateiformate

Beim Senden von Dateien muss das in der zu übertragenden Datei enthaltene Auftragsformat (z.B. "SEPA") zu der ausgewählten Auftragsart passen. So sollten zum Beispiel mit der Auftragsart "CCT - SEPA-Überweisungsdatei senden" lediglich XML-Dateien übertragen werden. Falls ein anderes Format mit dieser Auftragsart gesendet wird, wird der Auftrag zwar vom EBICS-Bankrechner entgegengenommen, er wird aber nicht weiterverarbeitet. Entsprechende Informationen können dem Kundenprotokoll (Auftragsarten "PTK" und "HAC") entnommen werden.

Tipp
Die Funktion "Inhalte analysieren" liefert Informationen zum jeweils vorliegenden Auftragsformat und kann somit unter Umständen die Wahl der Auftragsart erleichtern.

Nach der Datenübertragung

Wenn die Datenübertragung abgeschlossen ist, wird Ihnen das Ergebnis der Dateiübertragung zur Kontrolle angezeigt.

Diese Anzeige ist in der folgenden Abbildung beispielhaft dargestellt:

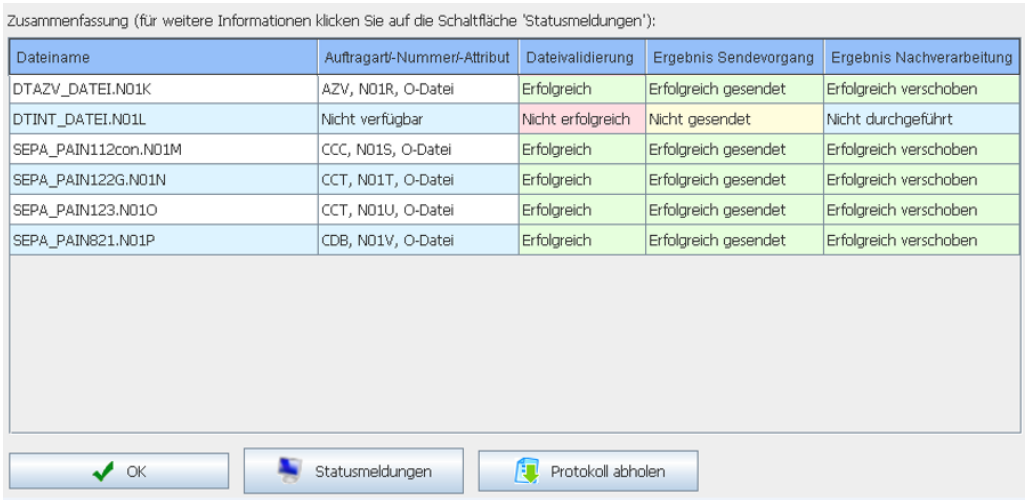


Abb. 5.2. Ergebnis der Datenübertragung

Über die Schaltfläche "Statusmeldungen" können die während des Übertragungsprozesses angezeigten Statusinformationen eingesehen werden. Im Folgenden wird die Bedeutung der einzelnen Tabellenspalten ersichtlich:

Spalte	Inhalt
Dateiname	Name der übertragenen Datei
Auftragsart / Nummer / Attribut	Es wird angegeben, mit welcher Auftragsart die Datei übertragen wurde und welche Auftragsnummer während der Datenübertragung vergeben wurde. Zudem wird ersichtlich, mit welchem Auftragsattribut die Datei gesendet wurde: • "O-Datei": Mit elektronischer Unterschrift • "D-Datei": Ohne elektronische Unterschrift • "Freigabe per Begleitzettel"

Spalte	Inhalt
Dateivalidierung	Es wird angegeben, ob die Dateivalidierung erfolgreich war. • "Erfolgreich": Das Auftragsformat wurde als fehlerfrei geprüft. • "Nicht erfolgreich": Das Auftragsformat wurde als nicht fehlerfrei geprüft.
Ergebnis Sendevorgang	Diese Spalte gibt das Ergebnis der EBICS-Datenübertragung wieder. **Anmerkung** Die Information bezieht auf den reinen Sendevorgang und nicht auf die Weiterverarbeitung auf dem Server.
Ergebnis Nachverarbeitung	Je nachdem, was in der Datenübertragungsmaske unter "Upload Optionen" eingestellt wurde, liefert diese Spalte das Ergebnis der lokalen Nachverarbeitung. **Tipp** Der Zielort verschobener Dateien ist das unter "Vorbelegungen" an der Zugangs-ID eingetragene "Transfered"-Verzeichnis.

Wie beschrieben liefert dieser Dialog lediglich Informationen über den technischen Ausgang einer Datenübertragung. Um in Erfahrung zu bringen, ob die gesendeten Dateien tatsächlich verarbeitet wurden, muss das dafür in EBICS vorgesehene Kundenprotokoll abgerufen werden. Näheres dazu finden Sie im Kapitel "Kontrollmöglichkeiten".

5.2.2. Dateien abholen

Bereitstellung von Download-Daten

Ebenso, wie Dateien an den EBICS-Bankrechner übertragen werden können, können auch Dateien bzw. Informationen vom jeweiligen EBICS-Bankrechner abgeholt werden. Hierzu stehen verschiedene Download-Auftragsarten zur Verfügung.

Damit Daten empfangen werden können, müssen diese zuvor am EBICS-Bankrechner für die entsprechende Auftragsart bereitgestellt worden sein.

Beispiel:

Es wurden Zahlungsaufträge verschiedener Auftragsarten an den EBICS-Bankrechner gesendet. Diese wurden erfolgreich verarbeitet und auf den entsprechenden Konten verbucht. Anschließend werden die gebuchten Umsätze im Format eines elektronischen Kontoauszugs (MT94x, CAMT) aufbereitet und als Download am EBICS-Bankrechner zur Verfügung gestellt. Die bereitgestellten Umsatzinformationen können über die entsprechende Auftragsart abgerufen werden.

Anmerkung

Es ist möglich, dass für die jeweilige Download-Auftragsart keine Daten zur Verfügung stehen. In diesem konkreten Beispiel wäre das der Fall, wenn am Vortag keine Umsätze auf den Konten des Kunden getätigt wurden.

Download-Auftragsart ausführen

Um eine Download-Auftragsart auszuführen, wechseln Sie auf den Reiter "Datenübertragung". Dort wählen Sie die Zugangs-ID aus, mit der die Daten abgeholt werden sollen.

Anschließend wählen Sie die Download-Auftragsart aus und geben den Speicherort für die empfangenen Daten an. Hierzu selektieren Sie das gewünschte Zielverzeichnis über den zur Verfügung stehenden Dateibaum.

Anmerkung
Für bestimmte Auftragsarten wird als Ablageort immer das an der Zugangs-ID konfigurierte "Dokumente"-Verzeichnis verwendet, damit die empfangenen Dokumente möglichst vollständig in einem Verzeichnis abgelegt werden. Dies ist im Abschnitt "Ablageort für Dokumente" beschrieben.

In der folgenden Abbildung ist der Reiter "Dateiübertragungen" dargestellt:

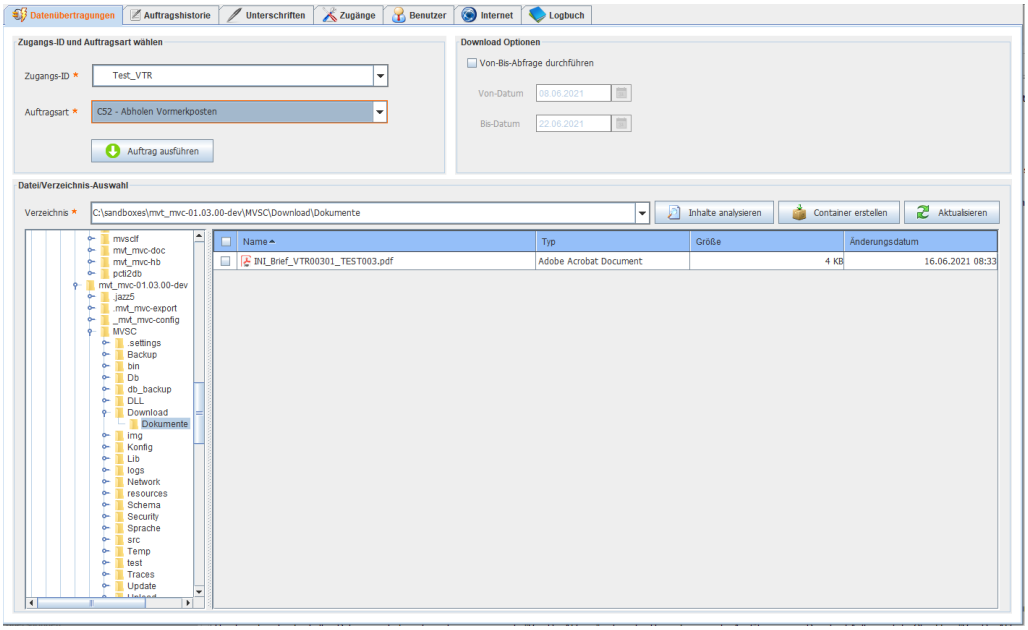


Abb. 5.3. Datei-Download

Historische Daten abrufen

Wenn am EBICS-Bankrechner bereitgestellte Download-Daten erstmalig abgeholt wurden, werden diese in den Status "Abgeholt" gesetzt. Sie stehen somit nicht mehr zum direkten Download zur Verfügung.

Um diese bereits abgeholten Daten erneut abzurufen, ist eine sogenannte "Von-Bis-Abfrage" notwendig. Hierzu kann vor der Ausführung einer Download-Auftragsart die Checkbox "Von-Bis-Abfrage" aktiviert werden. Ist das Kontrollkästchen aktiviert, muss über die darunterstehende Kalender-Auswahl der genaue Zeitraum der Abfrage definiert werden. Bei Betätigung der Schaltfläche "Auftrag ausführen" werden die Angaben an den jeweiligen EBICS-Bankrechner übermittelt. Dieser stellt die Daten gemäß dem angegebenen Zeitraum zusammen und liefert die für die Auftragsart gefundenen Daten zurück.

Anmerkung
Wie lange bestimmte Informationen über eine "Von-Bis-Abfrage" abrufbar sind, kann je nach EBICS-Bankrechner variieren. Somit ist es möglich, dass auch eine Von-Bis-Abfrage keine Informationen für den angegebenen Zeitraum liefert.

Ablageort für Dokumente

Als Speicherort für Dokumente ist für jede Zugangs-ID das unter "Vorbelegungen" hinterlegte "Dokumente"-Verzeichnis vorgesehen. In dem hier angegebenen Verzeichnis werden folgende Dokumente aufbewahrt:

- INI-Brief: Dieser enthält die während des Initialisierungsvorgangs ausgetauschten Schlüsselinformationen.
- Kundenprotokolle: Dies sind vom EBICS-Bankrechner heruntergeladene Protokolle, die Informationen über die Verarbeitung von gesendeten EBICS-Aufträgen enthalten. Derartige Protokolle können über zwei verschiedene Auftragsarten abgeholt werden:
  - Auftragsart "PTK": Diese Auftragsart liefert die Informationen in einem formatierten und aufbereiteten Format, das z.B. mit einem einfachen Texteditor lesbar ist.
  - Auftragsart "HAC": Diese Auftragsart enthält die Informationen im XML-Format, das maschinell ausgewertet und aufbereitet werden kann.

Achtung
Für die Auftragsarten "PTK" und "HAC" wird der in der Datenübertragungsmaske angegebene Speicherort ignoriert. Die Daten werden grundsätzlich im "Dokumente"-Verzeichnis der jeweils ausgewählten Zugangs-ID abgelegt.

5.2.3. Verteilte elektronische Unterschrift (im Nachfolgenden "VEU" genannt)

Auftragsarten und Unterschriftsklassen

Das EBICS-Verfahren bietet die Möglichkeit, Auftragsdateien im Vier- oder Mehr-Augen-Prinzip freizugeben. Dieses Verfahren kann nur in Kombination mit Upload-Auftragsarten zum Einsatz kommen, da für Download-Auftragsarten keine Unterschriftsklassen vergeben werden.

Folgende Unterschriftsklassen können am EBICS-Bankrechner vergeben werden:

Unterschriftsklasse	Beschreibung
T (Transportunterschrift)	Diese Unterschriftsklasse dient lediglich der Absicherung der Datenübertragung. Es können keine Aufträge freigegeben werden.
A (Erstunterschrift)	Diese Unterschriftsklasse ermöglicht die Auftragsfreigabe im Vier-Augen-Prinzip. Der Teilnehmer darf nur zusammen mit Teilnehmern der Unterschriftsklassen E, A oder B unterschreiben.
B (Zweitunterschrift)	Diese Unterschriftsklasse ermöglicht die Auftragsfreigabe im Vier-Augen-Prinzip. Der Teilnehmer darf nur zusammen mit Teilnehmern der Unterschriftsklassen E oder A unterschreiben.
E (Einzelvollmacht)	Bei dieser Unterschriftsklasse ist nur eine Unterschrift notwendig, um einen Auftrag endgültig freizugeben.

Da die Unterschriftsklasse je Teilnehmer auf der Ebene der Auftragsarten vergeben wird, ist es möglich, dass ein Teilnehmer für verschiedene Auftragsarten über unterschiedliche Unterschriftsklassen verfügt. Es könnte beispielsweise sein, dass ein Teilnehmer SEPA-Überweisungen alleine freigeben darf (E-Berechtigung für die Auftragsart "CCT"), aber Auslands-Aufträge im Vier-Augen-Prinzip (A bzw. B-Berechtigung für die Auftragsart "AZV") freigeben muss.

Beispiel zur Wertigkeit von Unterschriften

Zur Verdeutlichung der möglichen Rollenverteilung im Rahmen der VEU ist im Folgenden ein Beispiel zur Wertigkeit von Unterschriften dargestellt:

- Der Teilnehmer "BUCHHALT" ist ein Mitarbeiter in der Buchhaltung einer Firma. Seine Rolle ist es, die Auftragsdateien zu erstellen und diese zu übertragen. Für die Auftragsfreigabe sind andere Mitarbeiter zuständig.
- Der Teilnehmer "FREIGEB1" könnte in diesem Beispiel ein leitender Angestellter sein, der zusammen mit einem weiteren Mitarbeiter im Vier-Augen-Prinzip einen Auftrag freigeben darf.
- Der Teilnehmer "FREIGEB2" ist in der Lage, Aufträge von FREIGEB1 zu unterschreiben. Somit könnte er zusammen mit dem leitenden Angestellten einen Auftrag autorisieren.

- Der Teilnehmer "CHEFBOSS" wäre bei dieser Rollenverteilung der Geschäftsführer, der jederzeit in der Lage ist, einen Auftrag mit seiner alleinigen Unterschrift freizugeben.

Tabelle 5.1. Verdeutlichung der Rollenverteilung innerhalb der VEU

Teilnehmer-ID	Auftragsart	Unterschriftsklasse	Kombinationsmöglichkeiten
BUCHHALT	CCT	T	**Datenübertragung** Der Teilnehmer darf SEPA-Überweisungsdateien übertragen,- er hat aber kein Recht, diese freizugeben. Alle SEPA-Überweisungsdateien, die von diesem Teilnehmer übertragen werden, gelangen zunächst in die VEU. Für die Freigabe ist entweder eine Einzelvollmacht (E) notwendig oder es müssen 2 Teilnehmer mit A- bzw. B-Berechtigung unterschreiben.
FREIGEB1	CCT	A	**Datenübertragung** Der Teilnehmer darf SEPA-Überweisungsdateien mit A-Unterschrift übertragen. Diese von diesem Teilnehmer eingereichten SEPA-Überweisungsdateien sind nach Einreichung bereits mit einer A-Unterschrift versehen. Sie warten aber in der VEU auf weitere Unterschriften. Es wird nur eine weitere Unterschrift der Klasse A, B oder E benötigt, um den Auftrag endgültig freizugeben. **Verteilte elektronische Unterschrift (VEU)** Außerdem können SEPA-Überweisungsdateien anderer Teilnehmer, die auf weitere Unterschriften warten, durch diesen Teilnehmer mit einer A-Unterschrift versehen werden. Dies gilt zum Beispiel für SEPA-Überweisungsdateien, die von dem Teilnehmer "BUCHHALT" oder "FREIGEB2" eingereicht wurden.
FREIGEB2	CCT	B	**Datenübertragung** Der Teilnehmer darf SEPA-Überweisungsdateien mit B-Unterschrift übertragen. Diese von diesem Teilnehmer eingereichten SEPA-Überweisungsdateien sind nach Einreichung bereits mit einer B-Unterschrift versehen. Sie warten aber in der VEU auf weitere Unterschriften. Es wird nur eine weitere Unterschrift für die Freigabe benötigt, diese muss aber die Klasse A (Teilnehmer "FREIGEB1") oder E (Teilnehmer "CHEFBOSS") haben. Eine Freigabe mit zwei B-Unterschriften ist nicht möglich. **Verteilte elektronische Unterschrift (VEU)** Außerdem können SEPA-Überweisungsdateien, die auf weitere Unterschriften warten, durch diesen Teilnehmer mit einer B-Unterschrift versehen werden. Dies gilt zum Beispiel für SEPA-Überweisungsdateien, die von Teilnehmer "BUCHHALT" oder Teilnehmer "FREIGEB1" eingereicht wurden. SEPA-Überweisungsdateien, die zuvor jedoch nur mit einer B-Unterschrift versehen wurden, können durch diesen Teilnehmer nicht freigegeben werden.
CHEFBOSS	CCT	E	**Datenübertragung** SEPA-Überweisungsdateien, die von diesem Teilnehmer eingereicht werden, sind mit der Einreichung sofort vollständig autorisiert und somit freigegeben. Damit warten diese SEPA-Überweisungsdateien auch niemals in der VEU auf weitere Unterschriften, sondern werden direkt verarbeitet. **Verteilte elektronische Unterschrift (VEU)** Alle SEPA-Überweisungsdateien, die in der VEU auf weitere Unterschriften warten, können von diesem Teilnehmer direkt freigegeben werden. Dabei spielt es keine Rolle, ob die SEPA-Überweisungsdatei zuvor von Teilnehmer "BUCHHALT" (Unterschriftsklasse T), Teilnehmer

Teil-neh-mer-ID	Auf-trags-art	Unter-schrifts-klasse	Kombinationsmöglichkeiten
			"FREIGEB1" (Unterschriftsklasse A) oder Teilnehmer "FREIGEB2" (Unterschriftsklasse B) eingereicht wurde.

VEU-Übersicht abholen und bearbeiten

Um im Rahmen der verteilten elektronischen Unterschrift (VEU) weitere Unterschriften leisten zu können, muss zunächst die Übersicht der auf eine Unterschrift wartenden Aufträge vom EBICS-Bankrechner abgerufen werden. Hierfür steht Ihnen der Reiter "Unterschriften" zur Verfügung.

Es ist lediglich die Zugangs-ID auszuwählen, anschließend kann die Schaltfläche "Übersicht abholen" betätigt werden.

Nachdem die Übersicht erfolgreich abgeholt wurde, stehen Ihnen, sofern Aufträge geliefert wurden, weitere Funktionen zur Verfügung. Diese sind in der folgenden Tabelle beschrieben:

Funktion	Beschreibung
Stornieren	Die zuvor über die Kontrollkästchen ausgewählten Aufräge werden entfernt. Diese können dann auch von anderen Teilnehmern nicht mehr unterschrieben werden. **Achtung** Falls ein Auftrag irrtümlich storniert wurde ist eine Neueinreichung erforderlich.
Unterschreiben	Sie unterschreiben die zuvor über die Kontrollkästchen ausgewählten Aufträge.
Begleitzettel anzeigen	Der vom EBICS-Bankrechner aufbereitete Begleitzettel zur Auftragsdatei wird angezeigt. **Anmerkung** Die Anzeige weicht von der in MVSC integrierten Begleitzettel-Anzeige ab.
Auftragsdatei anzeigen	Die gesamte Auftragsdatei wird angezeigt.

In der folgenden Abbildung ist beispielhaft eine Übersicht von Aufträgen dargestellt:

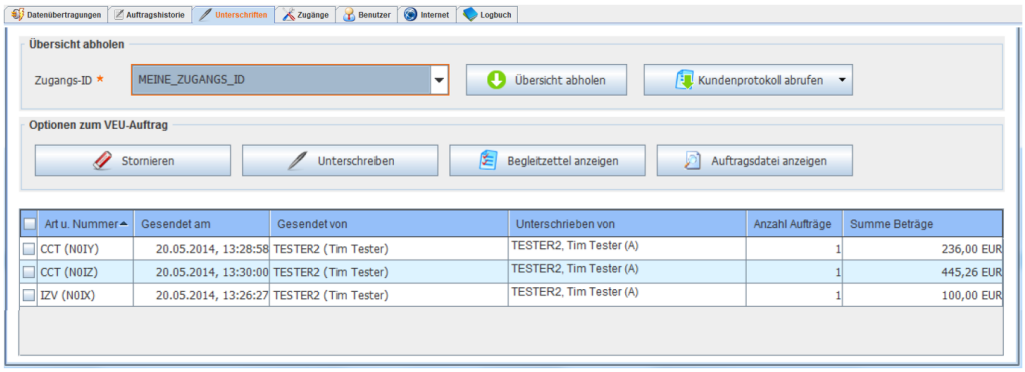


Abb. 5.4. Auftragsübersicht

5.2.4. Informationen zu Auftragsdateien

Dateiinhalte analysieren

Durch Betätigung der Schaltfläche "Inhalte analysieren" werden die in der Tabelle aufgelisteten Dateien auf gängige Auftragsformate geprüft.

In der folgenden Abbildung ist ein Dateiinhalt beispielhaft dargestellt:

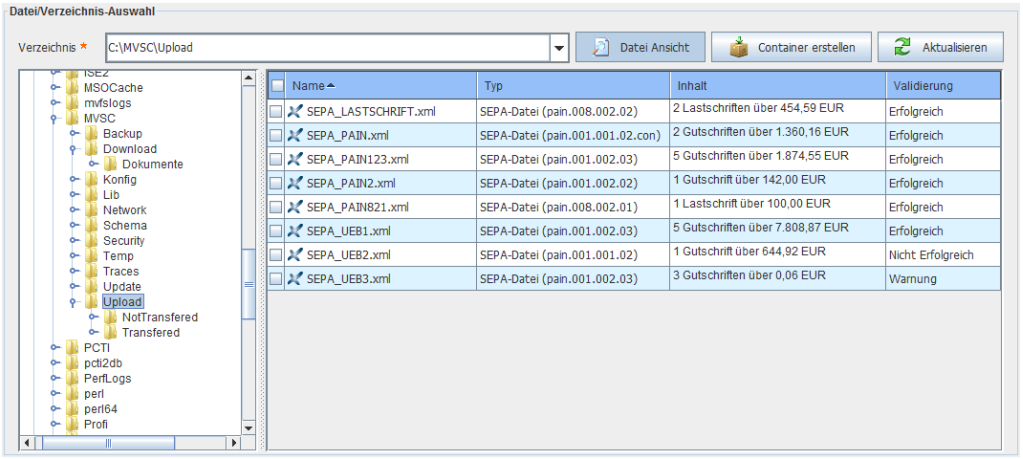


Abb. 5.5. Dateiinhalt

In der Spalte "Typ" wird das Format der jeweiligen Datei dargestellt. Die Spalte "Inhalte" liefert Informationen zu den in den Dateien enthaltenen Auftragsdaten. Die Spalte "Validierung" gibt an, ob das Format der Auftragsdaten korrekt ist.

Anmerkung

Die Prüfungen in dieser Ansicht sind identisch zu den Prüfungen, die während der Datenübertragung durchgeführt werden.

Auftragsdaten anzeigen

Per Doppelklick auf einen beliebigen Eintrag der Tabelle können Sie die Inhalte der ausgewählten Auftragsdatei einsehen.

In der folgenden Abbildung ist beispielhaft eine Zahlungsverkehrsdatei dargestellt:

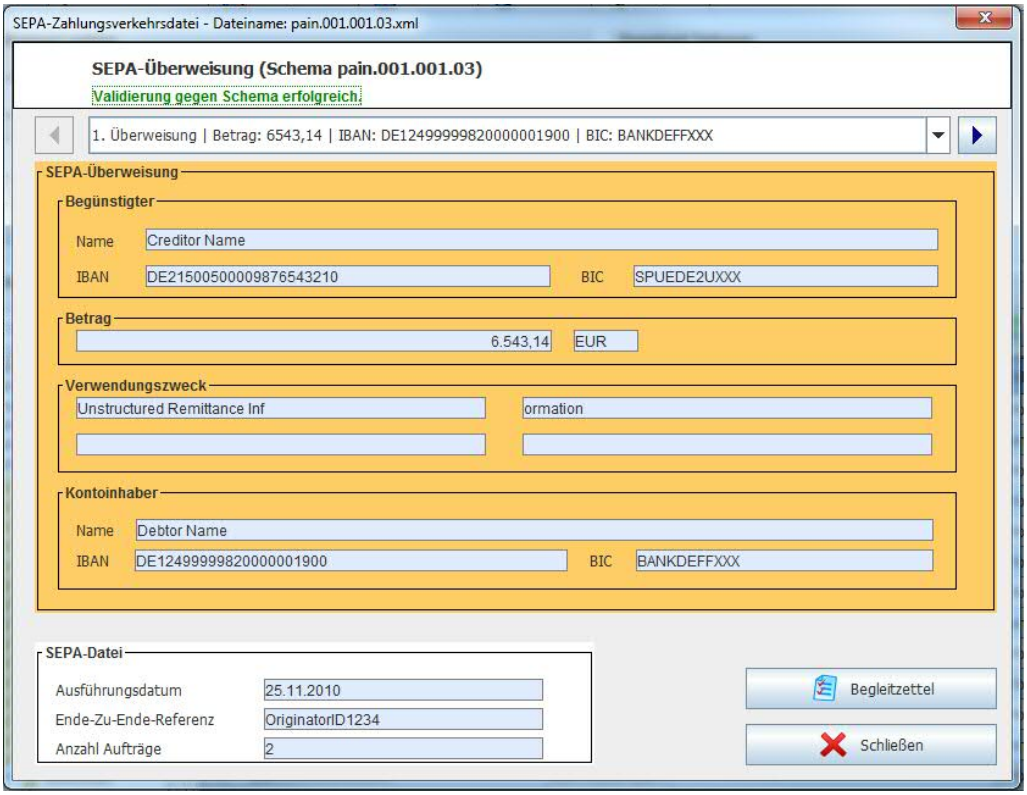


Abb. 5.6. Anzeige von Auftragsdaten

Die einzelnen Zahlungsaufträge können über die oben in der Maske positionierte Auswahlliste selektiert werden. Mit Hilfe der Schaltfläche "Begleitzettel" kann ein sogenannter "Datenträger Begleitzettel" erzeugt werden. Das Ergebnis der Dateivalidierung wird unterhalb der Überschrift in grün (Validierung erfolgreich) oder rot (Validierung fehlgeschlagen) dargestellt.

5.3. Kontrollmöglichkeiten

Protokollierung in EBICS

Jede Aktion (Upload/ Download von Daten) wird am EBICS-Bankrechnersystem protokolliert. Die im Protokoll enthaltenen Einträge und Ergebnisse geben letztlich Aufschluss über den Verarbeitungsstatus der jeweiligen Aktion bzw. der eingereichten Datei.

Das Protokoll kann über die Auftragsarten "PTK" oder "HAC" abgeholt und eingesehen werden. Inhaltlich sind beide Protokolle identisch, der Unterschied besteht in der Aufbereitung der Informationen.

PTK-Protokoll

Im PTK-Protokoll werden die einzelnen Verarbeitungsschritte von eingereichten Aufträgen **chronologisch** sortiert zurückgeliefert. Die Informationen sind in Blöcken aufbereitet. Dabei gibt jeder Block Auskunft über einen Verarbeitungsschritt. Es kann sein, dass zwischen den jeweiligen Verarbeitungsschritten weitere Aktionen stattgefunden haben, welche ebenfalls in das Protokoll eingetragen wurden. Das führt dazu, dass zwischen der Protokollierung der Einreichung und der letztendlichen Verarbeitung eines Auftrags Einträge zu anderen Aktionen enthalten sein können. Anhand der 4-stelligen Auftragsnummer (z.B. "N001") können Sie erkennen, zu welchem Auftrag der jeweilige PTK-Eintrag gehört.

In der folgenden Abbildung ist beispielhaft ein PTK-Protokoll dargestellt:

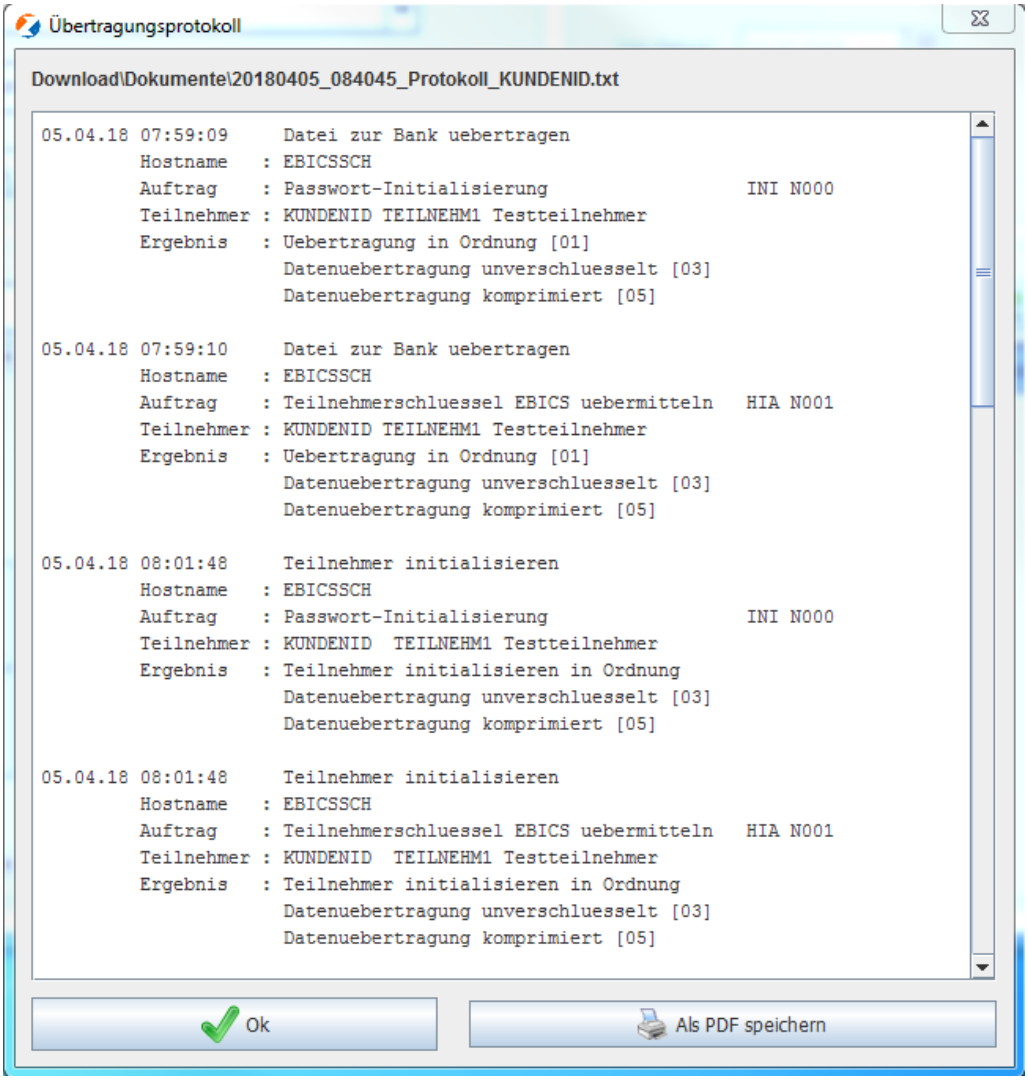


Abb. 5.7. PTK-Übertragungsprotokoll

HAC-Protokoll

Das HAC-Protokoll wurde mit EBICS-Version 2.5 eingeführt. Es liefert die aus dem PTK bekannten Informationen im XML-Format zurück. Der Vorteil liegt darin, dass die enthaltenen Rückmeldungen maschinell ausgewertet werden können. Die Anzeige in MVSC bietet Ihnen unter anderem die Möglichkeit, nach verschiedenen Kriterien zu sortieren.

Tipp
Durch die Sortierung über Auftragsart und Nummer können Sie die zu einer eingereichten Datei zugehörigen Einträge schneller finden.

Die Maske "HAC-Kundenprotokoll" ist in der folgenden Abbildung dargestellt:

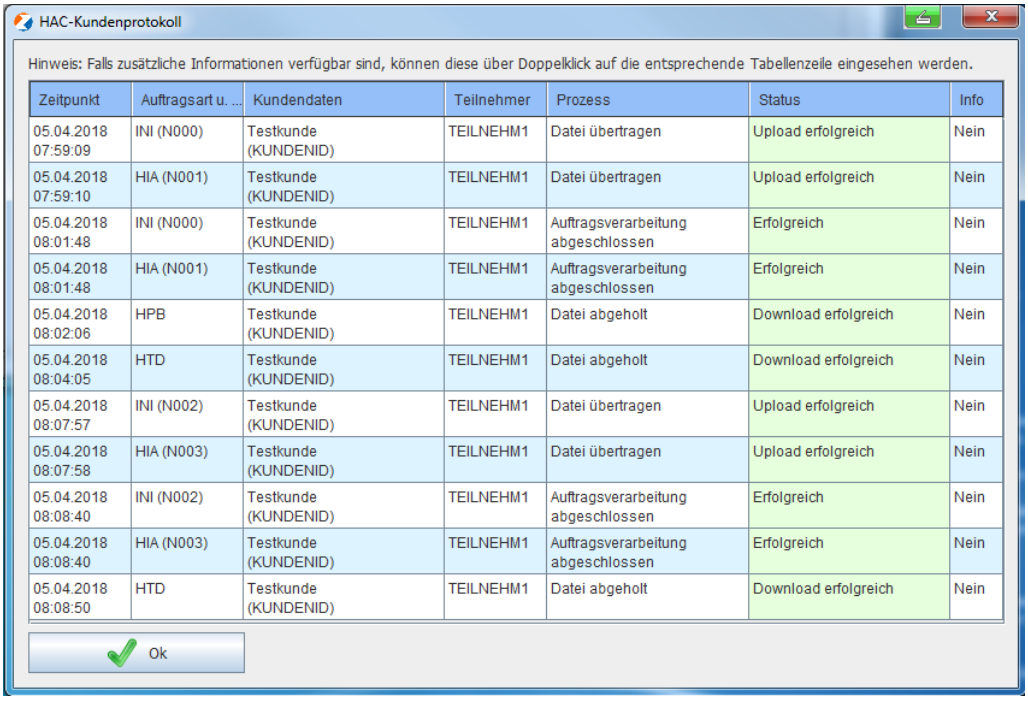


Abb. 5.8. HAC-Kundenprotokoll

Die aus dem PTK bekannten Begleitzettel können per Doppelklick eingesehen werden, wenn in der Spalte "Info" der Wert "Ja" eingetragen ist.

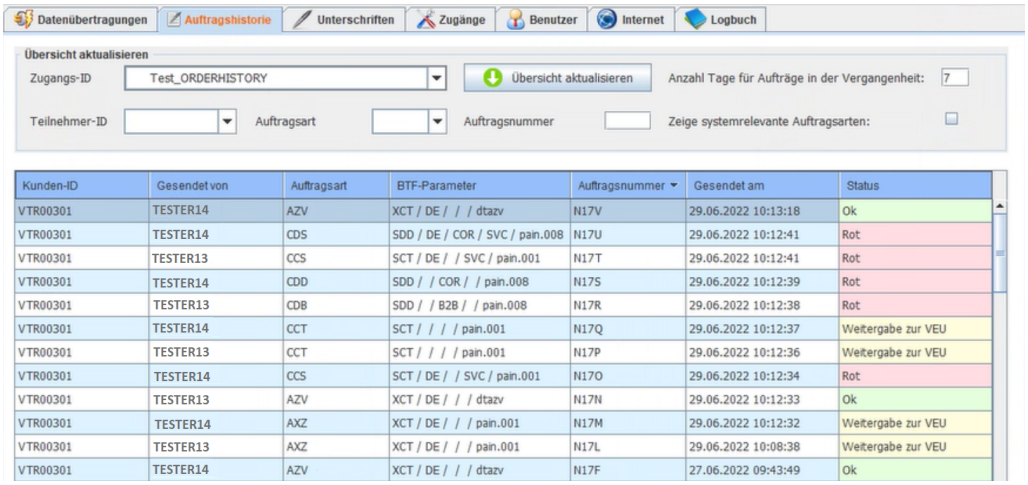
Wenn in der Spalte "Prozess" der Text "Auftragsverarbeitung abgeschlossen" enthalten ist, dann ist dies der letzte Protokoll-Eintrag zu dem jeweiligen Auftrag. Dieser Eintrag gibt letztendlich Auskunft über das Ergebnis der Verarbeitung.

Tipp
Die Einträge aus dem HAC-Protokoll werden Ihnen auch in der Auftragshistorie angezeigt. Näheres dazu finden Sie im folgenden Abschnitt "Auftragshistorie".

Auftragshistorie

In der Auftragshistorie werden Ihnen die Einträge des HAC-Protokolls zu den unterschiedlichen Auftragsarten wie zum Beispiel "AZV", "CCT" und "CDS" aufgelistet. Über das Kontrollkästchen "Zeige systemrelevante Auftragsarten" haben Sie dabei die Möglichkeit, die für das System relevante Auftragsarten ein- oder auszublenden. Jede Zeile der Auftragshistorie bezieht sich dabei auf einen Auftrag zur jeweiligen Kunden-ID und Zugangs-ID.

In der folgenden Abbildung ist die Maske "Auftragshistorie" beispielhaft dargestellt:



Kunden-ID	Gesendet von	Auftragsart	BTF-Parameter	Auftragsnummer	Gesendet am	Status
VTR00301	TESTER14	AZV	XCT / DE / / / dtazv	N17V	29.06.2022 10:13:18	Ok
VTR00301	TESTER14	CDS	SDD / DE / COR / SVC / pain.008	N17U	29.06.2022 10:12:41	Rot
VTR00301	TESTER13	CCS	SCT / DE / / SVC / pain.001	N17T	29.06.2022 10:12:41	Rot
VTR00301	TESTER14	CDD	SDD / / COR / / pain.008	N17S	29.06.2022 10:12:39	Rot
VTR00301	TESTER13	CDB	SDD / / B2B / / pain.008	N17R	29.06.2022 10:12:38	Rot
VTR00301	TESTER14	CCT	SCT / / / / pain.001	N17Q	29.06.2022 10:12:37	Weitergabe zur VEU
VTR00301	TESTER13	CCT	SCT / / / / pain.001	N17P	29.06.2022 10:12:36	Weitergabe zur VEU
VTR00301	TESTER14	CCS	SCT / DE / / SVC / pain.001	N17O	29.06.2022 10:12:34	Rot
VTR00301	TESTER13	AZV	XCT / DE / / / dtazv	N17N	29.06.2022 10:12:33	Ok
VTR00301	TESTER14	AXZ	XCT / DE / / / pain.001	N17M	29.06.2022 10:12:32	Weitergabe zur VEU
VTR00301	TESTER13	AXZ	XCT / DE / / / pain.001	N17L	29.06.2022 10:08:38	Weitergabe zur VEU
VTR00301	TESTER14	AZV	XCT / DE / / / dtazv	N17F	27.06.2022 09:43:49	Ok

Abb. 5.9. Auftragshistorie

Betätigen Sie die Schaltfläche "Übersicht aktualisieren", um die Tabelle der Auftragshistorie auf der Grundlage des HAC-Protokolls zu füllen bzw. zu aktualisieren.

Über das Feld "Anzahl Tage für Aufträge in der Vergangenheit" legen Sie den Zeitrahmen fest, für den die Auftragshistorie aktualisiert wird. Möglich ist hier eine Angabe zwischen 1 und 90 Tagen.

Anschließend haben Sie per Doppelklick auf eine Zeile die Möglichkeit, sich Zusatzinformationen zu dem jeweiligen Auftrag anzeigen zu lassen.

In der folgenden Abbildung sind beispielhaft Zusatzinformationen zu einem Auftrag dargestellt:

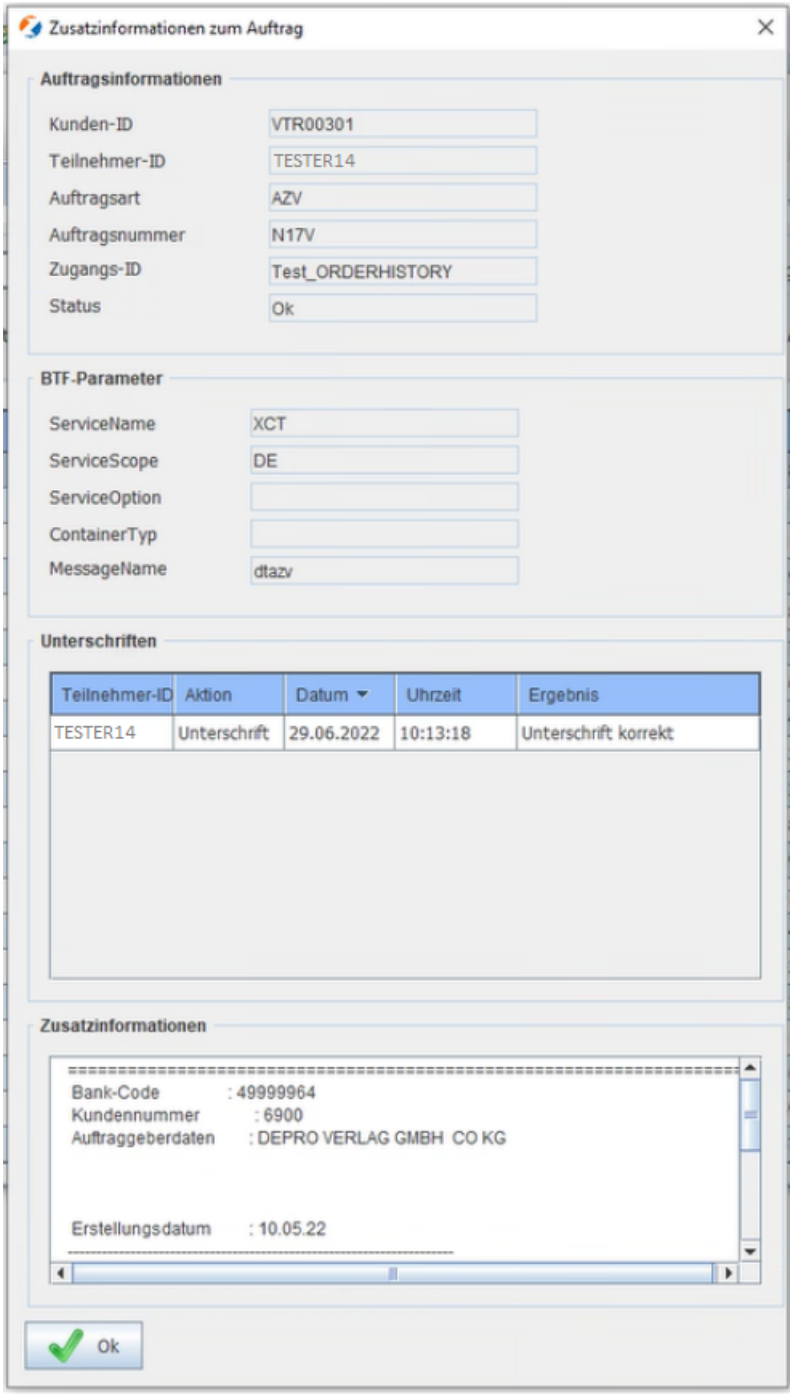


Abb. 5.10. Aufragshistorie - Zusatzinformationen zum Auftrag

In den Einstellungen legen Sie fest, nach welchem Zeitraum die Auftragshistorie geleert wird. Sie finden die Einstellungen im Menü unter dem Menüpunkt "Konfiguration", "Einstellungen".

Der Aufruf der Einstellungen ist in der folgenden Abbildung dargestellt:

Abb. 5.11. Auftragshistorie - Aufruf der Einstellungen

In der folgenden Abbildung sind die Einstellungen mit der Angabe "Wartezeit in Tagen bis die Auftragshistorie geleert wird" dargestellt:

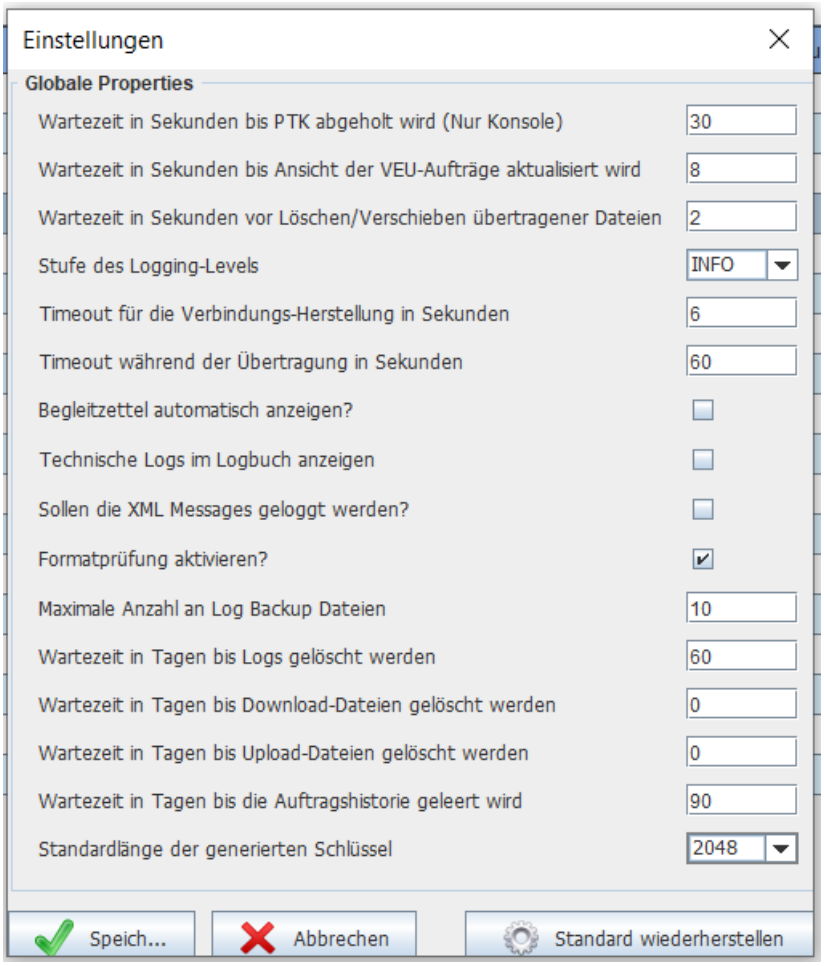


Abb. 5.12. Auftragshistorie - Einstellungen

Diese Angabe "Wartezeit in Tagen, bis die Aufragshistorie geleert wird" ist in Abhängigkeit zum Auftragsvolumen und zur Nutzungshäufigkeit sinnvoll zu wählen. Ältere Einträge werden dann nach erfolgter Aktualisierung über die Schaltfläche "Übersicht aktualisieren" nicht mehr in der Auftragshistorie angezeigt. Sie können aber (abhängig vom Feld "Anzahl Tage für Aufträge in der Vergangenheit") durch Änderung der Angabe und erneuter Aktualisierung der Übersicht wieder aufgenommen werden.

Tipp
Beachten Sie aber, dass Aufträge, die älter als 90 Tage sind und einmal aus der Auftragshistorie entfernt wurden, nicht wieder aufgenommen werden können.

Die Angabe von 0 Tagen bedeutet, dass alle vorhandenen Aufträge aus der Auftragshistorie angezeigt werden. Standardmäßig werden 90 Tage voreingestellt.

Aufträge, die aus der Auftragshistorie entfernt werden, werden automatisch in eine CSV-Datei exportiert, die im Download-Verzeichnis gespeichert wird. Näheres zur Angabe des Download-Verzeichnisses in den Standardeinstellungen finden Sie im Kapitel "Vorbelegungen".

5.4. Nutzung in der Konsole

Voraussetzungen

Nachdem alle Verbindungsdaten (EBICS und Internet) korrekt in MVSC erfasst wurden, ist die Nutzung in der Konsole durch einen einfachen Aufruf realisierbar. Voraussetzung dafür ist jedoch, dass die Passwörter für Sicherheitsmedium und ggf. Proxy-Authentifizierung im Programm gespeichert sind.

Anmerkung
Die Verwendung des Konsolenmodus ist nur mit Zugangs-IDs möglich, bei denen als Sicherheitsmedium eine Sicherheitsdatei hinterlegt wurde.

Vorbereitungen

Bevor der Konsolenmodus verwendet wird, sollten einige Einstellungen kontrolliert werden:

- Ist die Zugangs-ID bereits vollständig initialisiert worden?
- Wird als Sicherheitsmedium eine Sicherheitsdatei verwendet?
- Ist das Passwort für die Sicherheitsdatei an der Zugangs-ID hinterlegt worden?
- Sind die Einstellungen im Dialog "Vorbelegungen" korrekt?
- Wird die Internetverbindung über einen Proxy-Server hergestellt und sind ggf. notwendige Authentifizierungs-Informationen unter dem Reiter "Internet" hinterlegt?

Wenn diese Voraussetzungen erfüllt sind, kann ein Konsolenaufruf durchgeführt werden.

Anmerkung
Um in den Dialog "Vorbelegungen" zu gelangen, wechseln Sie auf den Reiter "Zugänge". Wählen Sie die Zugangs-ID aus, mit der ein Konsolenaufruf realisiert werden soll, und betätigen Sie die Schaltfläche "Vorbelegungen".

Aufruf aus der Konsole

Sind alle im Vorfeld genannten Bedingungen erfüllt, öffnen Sie Ihre Konsole (Start->Ausführen->cmd) und wechseln Sie in das MVSC-Installationsverzeichnis:

```
cd C:\Installations\Verzeichnis\MVSC\
```

Starten Sie MVSC mit mindestens einem Aufrufparameter (Name der Zugangs-ID, mit der Daten übertragen bzw. abgeholt werden sollen).

Folgende Aufrufvarianten stehen zur Verfügung:

1. **Variante A: Es wird nur die Zugangs-ID übergeben, alle anderen Parameter werden aus der hinterlegten Konfiguration ermittelt.**

   ```
   LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID"
   ```

   Die für diese Zugangs-ID unter "Zugänge->Vorbelegungen" eingestellte Auftragsart wird ausgeführt.

   Wurde eine Upload-Auftragsart hinterlegt, so werden alle Dateien übertragen, die im eingestellten Upload-Verzeichnis dem für die Auftragsart konfigurierten Dateifilter entsprechen.

   Ist eine Download-Auftragsart hinterlegt worden, so werden die empfangenen Daten im angegebenen Download-Verzeichnis (oder Dokumenten-Verzeichnis) gespeichert.

2. **Variante B: Die Zugangs-ID und die Auftragsart werden übergeben.**

```
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" "Auftragsart"
```

Die übergebene Auftragsart wird ausgeführt. Auch hier wird im Falle eines Uploads der für die übergebene Auftragsart konfigurierte Dateifilter auf das hinterlegte Upload-Verzeichnis angewandt (vgl. Variante A).

3. **Variante C: Die Zugangs-ID, die Auftragsart und das Upload- bzw. Download-Verzeichnis müssen angegeben werden. Bei Upload-Auftragsarten können zusätzlich optional ein Aktionsparameter und zwei Verzeichnisse angegeben werden.**

```
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" "Auftragsart"
 "Pfad/zum/Verzeichnis"
```

Die übergebene Auftragsart wird ausgeführt.

Bei Upload-Auftragsarten wird der dritte Parameter als Upload-Verzeichnis interpretiert. Das bedeutet, der für die Auftragsart gültige Dateifilter wird auf diesen Verzeichnispfad angewandt.

Wird eine Download-Auftragsart übergeben, so werden die empfangenen Daten in dem übergebenen Zielverzeichnis abgelegt.

Anmerkung
Für die Auftragsarten "HAC" und "PTK" wird der übergebene Pfad ignoriert,- stattdessen wird das Dokumenten-Verzeichnis als Speicherort verwendet.

Zusätzlich können bei Upload-Auftragsarten optional ein Aktionsparameter und zwei Verzeichnisse angegeben werden.

In diesem Fall sieht der Aufruf wie folgt aus:

```
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" "Auftragsart"
 "Pfad/zum/Verzeichnis" "-Aktionsparameter" "Pfad/zum/Verschieben"
"Pfad/bei/fehlerhafter/Uebertragung"
```

Der optionale Aktionsparameter kann die folgenden Werte annehmen:

Aktionsparameter	Bedeutung
"-verschieben"	Erfolgreich übertragene Dateien werden in das Verzeichnis "Pfad/zum/Verschieben" verschoben. Wird dieses Verzeichnis beim Aufruf nicht angegeben, so werden die Einstellungen aus den Vorbelegungen verwendet.
"-loeschen"	Erfolgreich übertragene Dateien werden gelöscht. Ein angegebener Pfad zum Verschieben wird ignoriert.
"-keineAktion"	Die übertragenen Dateien werden weder verschoben noch gelöscht. Ein angegebener Pfad zum Verschieben wird ignoriert.

Sollte es bei der Übertragung der Datei zu einem Fehler kommen, so wird die zu übertragende Datei in das Verzeichnis "Pfad/bei/fehlerhafter/Uebertragung" verschoben.

Wird dieses Verzeichnis beim Aufruf nicht angegeben, so werden die Einstellungen aus den Vorbelegungen verwendet.

4. **Variante D: Die Zugangs-ID, die Auftragsart und die Datei (Upload- oder Download-Datei) werden übergeben. Diese Variante gibt es in zwei Versionen, einmal für Upload-Auftragsarten und einmal für Download-Auftragsarten.**
Upload-Auftragsarten:

```
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" "Auftragsart"
 "Pfad/zur/Upload-Datei"
```

Die übergebene Datei wird unter Berücksichtigung der angegebenen Zugangs-ID und Auftragsart übertragen. Die Datei wird bei diesem Aufruf weder verschoben noch gelöscht.

Zusätzlich können aber optional ein Aktionsparameter und zwei Verzeichnisse angegeben werden.

In diesem Fall sieht der Aufruf wie folgt aus:

```
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" "Auftragsart"
 "Pfad/zur/Upload-Datei" "-Aktionsparameter" "Pfad/zum/Verschieben"
"Pfad/bei/fehlerhafter/Uebertragung"
```

Der optionale Aktionsparameter kann folgende Werte annehmen:

Aktionsparameter	Bedeutung
"-verschieben"	Erfolgreich übertragene Dateien werden in das Verzeichnis "Pfad/zum/Verschieben" verschoben. Wird dieses Verzeichnis beim Aufruf nicht angegeben, so werden die Einstellungen aus den Vorbelegungen verwendet.
"-loeschen"	Erfolgreich übertragene Dateien werden gelöscht.
"-keineAktion"	Die übertragenen Dateien werden weder verschoben noch gelöscht. Ein angegebener Pfad zum Verschieben wird ignoriert.

Sollte es bei der Übertragung der Datei zu einem Fehler kommen, so wird die zu übertragende Datei in das Verzeichnis "Pfad/bei/fehlerhafter/Uebertragung" verschoben.

Wird dieses Verzeichnis beim Aufruf nicht angegeben, so werden die Einstellungen aus den Vorbelegungen verwendet.

Download-Auftragsarten:

Für Download-Auftragsarten (z.B. "AUTD") gibt es zwei Möglichkeiten, wie der Aufruf erfolgen kann.

Standardmäßig ist der Aufruf

```
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" "Auftragsart
 Download"
```

zu verwenden.

Alternativ, insbesondere wenn Kontoumsätze für ein spezielles Datum oder für einen speziellen Zeitraum abgeholt werden sollen, kann der folgende Aufruf verwendet werden:

```
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" "Auftragsart
 Download" "Pfad/zum/Download-Verzeichnis" "Aktionsparameter"
```

Die beiden Parameter "Pfad zum Downloadverzeichnis" und "Aktionsparameter" sind somit optional.

Die folgenden Aktionsparameter können alternativ verwendet werden:

Aktionsparameter	Bedeutung
"-Datum="	Bei Kontoumsätzen ist das Datum "von", "bis" in der Form "tt.mm.jjjj,tt.mm.jjjj" einzutragen. Beispiel: "-Datum=30.09.2024,15.10.2024" Es werden in diesem Beispiel die Kontoumsätze einschließlich vom 30.09. bis einschließlich zum 15.10. abgerufen.
"-Zeitraum="	Bei Kontoumsätzen ist hier die Angabe der beiden Zahlwerte "Anzahl der Tage von" und "Anzahl der Tage bis" einzutragen. Die erste Zahl entspricht dabei dem Startpunkt (Anzahl der Tage in der Vergangenheit), die zweite Zahl entspricht dem Endpunkt (Anzahl der Tage in der Vergangenheit).

Aktionsparameter	Bedeutung
	Beispiel: "-Zeitraum=2,1": Diese Angabe beinhaltet die Tage "vorgestern" und "gestern". Beispiel: "-Zeitraum=2,0": Diese Angabe beinhaltet die Tage "vorgestern", "gestern" und "heute". Beispiel: "-Zeitraum=0,0": Diese Angabe beinhaltet nur den heutigen Tag.

Empfohlen wird die Angabe des Zeitraums.

Auftragsarten "AUTO" und "AUTD"

Bei der Upload-Auftragsart "AUTO" werden alle Uploaddateien aus dem jeweiligen Uploadverzeichnis mit der entsprechenden Auftragsart des Auftrags zum Bankrechner übertragen.

Anmerkung
Wird im Unterschied dazu zum Beispiel die Auftragsart "CCT" angegeben, so werden nur Dateien mit der Auftragsart "CCT" übertragen.

Bei der Download-Auftragsart "AUTD" werden alle Downloadauftragsarten, die für die angegebene Zugangs-ID gültig sind, durchgeführt.

(Beispiel: 'LibJAV\bin\java MVSC.jar ZugangsIdTest1 AUTD c:\MVSC\Download\ ')

Ein einzelner Aufruf von CAMT- oder MT940-Kontoumsatzdaten ist somit nicht nötig.

Tipp
Möchten Sie, dass im Batch-Modus keine PTK-/HAC-Datei beim Download erstellt wird, so können Sie den entsprechenden Eintrag in der "Db\mvsc.properties" auf "ON" setzen ("hac.before.download=ON"). Standardmäßig steht dieser Wert auf "OFF".

Ablauf

Es sind anschließend keine weiteren Angaben mehr möglich oder nötig. MVSC erkennt die übergebene Zugangs-ID und sucht im angegebenen Uploadverzeichnis nach Dateien, die dem konfigurierten Dateifilter für die Auftragsart entsprechen. Diese werden nacheinander an das EBICS-Bankrechnersystem übertragen.

Achtung
Wenn das Programm zyklisch (z.B. alle 30 Minuten) aufgerufen wird, muss dafür gesorgt werden, dass bereits übertragene Dateien nicht mit dem nächsten Programmaufruf erneut übertragen werden. Es wird deshalb empfohlen, die Dateien von MVSC verschieben oder löschen zu lassen. Andernfalls muss der Aufrufer selbst dafür sorgen, dass Dateien nicht mehrfach übertragen werden.

Rückgabe

Nach Abschluss der Übertragungen gibt MVSC einen Wert zurück, der Aufschluss darüber gibt, ob die Aktion erfolgreich war. Näheres über die einzelnen Rückgabewerte finden Sie im Kapitel "Rückgabewerte im Konsolenmodus".

Tipp
Die während der Übertragung auf der Konsole ausgegebenen Informationen können über das Betriebssystem in eine Datei umgeleitet werden. Hierfür muss diese Zieldatei hinter dem jeweiligen MVSC-Aufruf entweder zum Überschreiben mit einem ">"-Zeichen oder zum Fortschreiben mit zwei ">"-Zeichen angegeben werden.

Beispiel: "Aufrufvariante >> MVSC_Aufruf.log"

5.5. Automatisierte Nutzung mit Hilfe einer Batch-Datei

Integration in komplexe Verarbeitungen

Wenn MVSC als Übertragungskomponente in einen komplexen Gesamtvorgang eingebaut werden soll, ist dies zum Beispiel über eine sogenannte Batch-Datei realisierbar. Der Aufruf der Anwendung erfolgt dann aus einem selbst zu erstellenden Rahmenprogramm, das einen mehr oder weniger komplexen Vorgang automatisiert bearbeitet.

Ein relativ einfaches Beispiel wird in der folgenden Tabelle beschrieben:

Aktion	Vorgang/Ergebnis
Aufruf einer Buchhaltungssoftware	Es wurden Zahlungsverkehrsdateien mit der Dateiendung ".xml" in einem definierten Ausgangsverzeichnis erzeugt.
Aufruf MVSC (entspricht Variante B der Aufrufvarianten)	**Voraussetzung gemäß Variante B:** Als Aufrufparameter werden MVSC die Zugangs-ID sowie die Auftragsart übergeben. Das Ausgangsverzeichnis wurde zuvor an der Zugangs-ID als Upload-Verzeichnis vorbelegt. Für die übergebene Auftragsart wurde darüber hinaus im Dateifilter die Dateiendung ".xml" eingetragen. **Ergebnis des Aufrufs:** Alle Dateien, die innerhalb des Ausgangsverzeichnisses die Dateiendung ".xml" tragen, werden mit der übergebenen Zugangs-ID an den EBICS-Bankrechner übertragen.
Abfrage des MVSC Rückgabewerts	Der von MVSC zurückgelieferte Wert muss ausgewertet werden. Anhand dieses Werts kann bestimmt werden, wie im Gesamtprozess fortgefahren werden soll.

Beispiel für eine Batch-Datei

Mit MVSC wurde bereits eine Batch-Datei ausgeliefert. Diese trägt den Namen "beispiel_batch.cmd" und befindet sich im MVSC-Installationsverzeichnis.

Die Datei soll lediglich als Beispiel dienen und ist in der ausgelieferten Form nicht lauffähig. In dem beigefügten Beispiel wird MVSC vom Zeitpunkt des Aufrufs bis 23 Uhr abends alle 10 Minuten einmal aufgerufen. Anschließend werden bestimmte Rückgabewerte des Programms ausgewertet und ausgegeben.

Folgende Zeile muss angepasst werden, damit die Datei ausgeführt werden kann (Zeile 46 in der Datei):

```
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" <$MEINE_ZUGANGSID>
<$MEINE_AUFTRAGSART> <$MEIN_UPLOADVERZEICHNIS>
```

Hier müssen noch die Zugangs-ID, die Auftragsart und das Upload-Verzeichnis angepasst werden. Selbstverständlich kann auch eine andere Aufrufvariante eingetragen werden.

5.6. Vorbelegungen

Allgemeines

Der Dialog "Vorbelegungen" dient hauptsächlich zur Konfiguration des Konsolenmodus. Hier werden z.B. die Verzeichnisse festgelegt, in denen das Programm bei entsprechendem Aufruf nach Dateien eines bestimmten Musters sucht.

Darüber hinaus bietet der Dialog einige Einstellungen, die auch auf die Nutzung im Dialog Auswirkungen haben.

Abbildung des Dialogs

In der folgenden Abbildung ist die Maske "Standardeinstellungen vorbelegen" dargestellt:

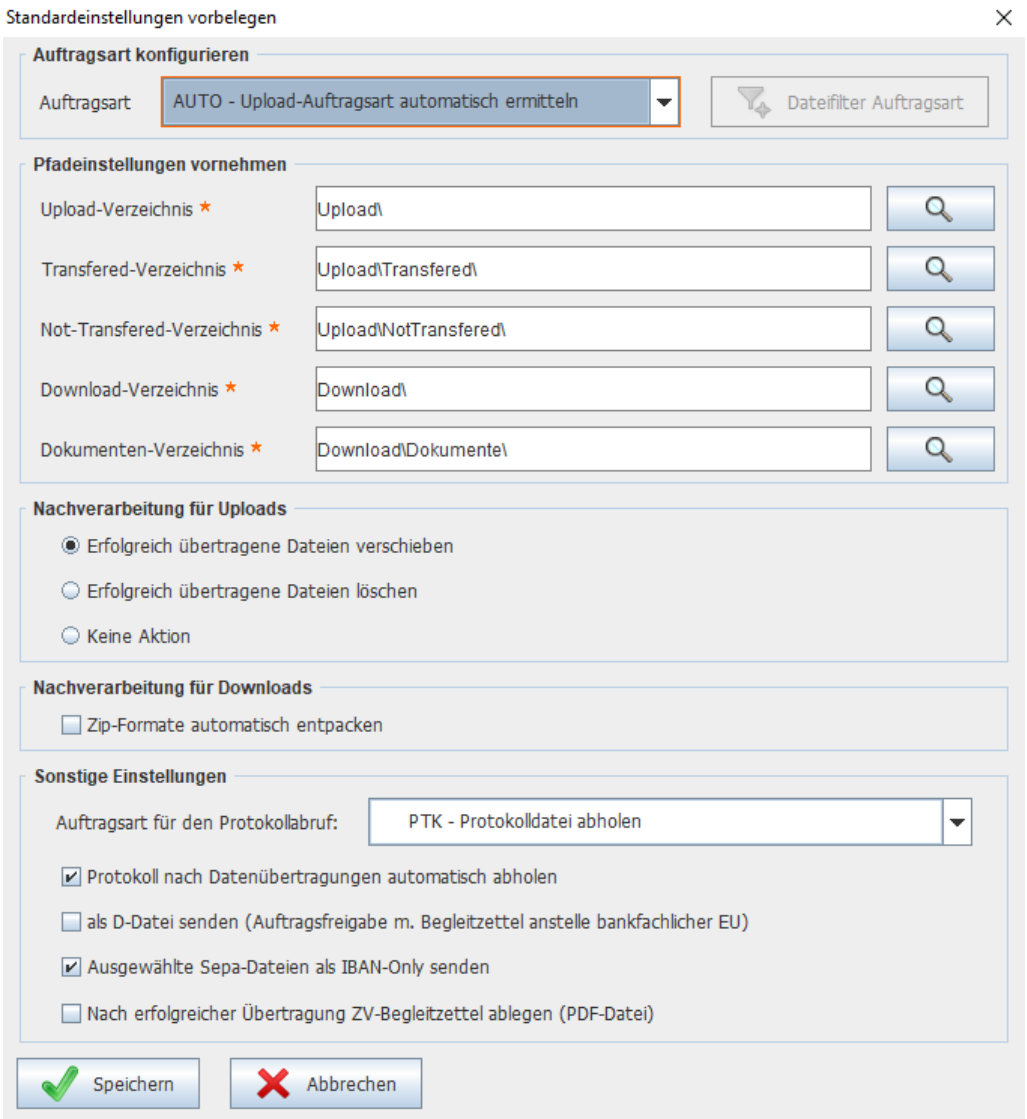


Abb. 5.13. Standardeinstellungen vorbelegen

Gruppierung "Auftragsart konfigurieren"

Die im Auswahlfeld eingestellte Auftragsart wird ausgeführt, wenn der Anwender das Programm im Konsolenmodus mit der entsprechenden Zugangs-ID als Übergabeparameter aufruft. Wurde eine Upload-Auftragsart ausgewählt, ist die Schaltfläche "Dateifilter Auftragsart" aktiviert. Bei Betätigung dieser Schaltfläche öffnet sich der sogenannte "Dateifilter-Editor". Hier können Sie Dateiendungen (z.B. "txt") hinterlegen, die mit der aktuell ausgewählten Auftragsart übertragen werden sollen.

Gruppierung "Pfadeinstellungen vornehmen"

An dieser Stelle werden die Ablageverzeichnisse für die ausgewählte Zugangs-ID definiert.

- **Upload-Verzeichnis:**
  Dieses Verzeichnis wird bei Programmaufruf mit dem Übergabeparameter "Zugangs-ID" nach Dateien durchsucht, die dem eingestellten Dateifilter der jeweiligen Auftragsart entsprechen. Alle Dateien, die gemäß diesem Filter gefunden werden, werden automatisch mit dieser Auftragsart übertragen.

In der Maske "Datenübertragungen" wird dieses Verzeichnis vorbelegt, wenn eine Upload-Auftragsart ausgewählt wurde.

- **Transfered-Verzeichnis:**
  Dateien, die durch MVSC übertragen wurden, werden in dieses Verzeichnis verschoben, damit sie bei erneutem Aufruf des Programms nicht mehrfach übertragen werden können.
- **Not-Transfered-Verzeichnis:**
  Dateien, die im Konsolenmodus nicht erfolgreich übertragen werden konnten, werden in dieses Verzeichnis verschoben. Im Oberflächen-Modus bleiben nicht erfolgreich übertragene Dateien an ihrem ursprünglichen Speicherort. Das Verzeichnis ist also nur im Konsolenmodus relevant.
- **Download-Verzeichnis:**
  In diesem Verzeichnis werden alle Dateien abgelegt, die über eine Download-Auftragsart empfangen wurden. Ausgenommen sind hierbei die Informationen aus den Auftragsarten "PTK" (Protokolldatei abholen) und die des Initialisierungsvorgangs (INI-Briefe).

  Das Download-Verzeichnis wird in der Maske "Datenübertragungen" vorbelegt, wenn eine Download-Auftragsart ausgewählt wurde.
- **Dokumenten-Verzeichnis:**
  Hier werden die vom Bankrechner abgeholten Protokolldateien (Auftragsart "PTK") abgelegt. Außerdem dient dieses Verzeichnis als Ablageort für die INI-Briefe.

Gruppierung "Nachverarbeitung für Uploads"

Nachdem eine Datei an den EBICS-Bankrechner übertragen wurde, gibt es insgesamt drei Möglichkeiten, wie mit der Datei umgegangen werden soll:

- "Erfolgreich übertragene Dateien verschieben": Die Datei wird in das angegebene Transfered-Verzeichnis verschoben. (Standard)
- "Erfolgreich übertragene Dateien löschen": Die übertragene Datei wird gelöscht.
- "Keine Aktion": Es wird keine Nachverarbeitung durchgeführt, die übertragene Datei bleibt bestehen.

Die ausgewählte Nachverarbeitung wird nur durchgeführt, wenn die Datei zuvor erfolgreich an den EBICS-Bankrechner übertragen wurde.

Achtung
Wenn im Konsolenmodus gearbeitet wird, sollten die Dateien möglichst verschoben oder gelöscht werden, da diese sonst beim nächsten Programmaufruf erneut übertragen werden könnten. Wurde "Keine Aktion" ausgewählt, dann muss der aufrufende Prozess sicherstellen, dass Dateien nicht mehrfach übertragen werden können.

Gruppierung "Nachverarbeitung für Downloads"

Wenn die Option "Zip-Formate automatisch entpacken" aktiviert ist, werden Download-Dateien im Zip-Format (z.B. CAMT-Dateien) automatisch von MVSC entpackt.

Dabei wird immer ein Unterverzeichnis erzeugt, das den gleichen Namen erhält, wie die Download-Datei ohne Dateiendung.

Beispiel:

Wenn eine Datei unter dem Namen "C53_20131216_135056_KUNDENID_TEILNEHMERID.C53" gespeichert wurde, wird sie in das Verzeichnis "C53_20131216_135056_KUNDENID_TEILNEHMERID" entpackt.

Gruppierung "Sonstige Einstellungen"

Diese Einstellungen gelten sowohl im Konsolenmodus als auch für Datenübertragungen aus der Benutzeroberfläche heraus:

- **Auftragsart für den Protokollabruf:**
  Ab der EBICS-Version 2.5 gibt es für den Abruf des Kundenprotokolls zwei Auftragsarten: "PTK" und "HAC". Während die Auftragsart "PTK" das Protokoll in textlich aufbereiteter Form zurückliefert, liefert die Auftragsart "HAC" die identischen Informationen im maschinell auswertbaren XML-Format.

  In diesem Feld wird angegeben, mit welcher Auftragsart und damit in welchem Format das Kundenprotokoll abgeholt werden soll.

  Anmerkung
  Sollte die Auftragsart "HAC" bei der jeweiligen Zugangs-ID nicht zugeordnet sein, so ist die Auswahlliste deaktiviert. Es wird dann die Auftragsart "PTK" verwendet.

- **Protokoll nach Datenübertragungen automatisch abholen:**
  Im Konsolenmodus wird nach Übertragung der Auftragsdateien automatisch das Kundenprotokoll abgerufen. Diese Option hat keine Auswirkungen auf den Betrieb mit der Benutzeroberfläche.
- **Als D-Datei senden:**
  Über diese Option können Sie Dateien ohne elektronische Unterschrift (EU) an den Bankrechner übertragen. Die so übertragenen Aufträge müssen durch einen unterschriebenen Begleitzettel, der in Papierform bei der Bank vorzulegen ist, freigegeben werden.
- **Ausgewählte Sepa-Dateien als IBAN-Only senden:**
  Ist dieses Kontrollkästchen aktiviert, so werden bei der Übertragung einer SEPA-Datei alle darin enthaltenen BICs entfernt. Die Originaldatei befindet sich anschließend im Verzeichnis "Upload/Original". Die übertragene Datei befindet sich dagegen anschließend im Verzeichnis "Upload/Transfered".

  Achtung
  Diese Option wird bei der Datenübertragung automatisch voreingestellt. Die Voreinstellung kann aber manuell zurückgenommen werden.

- **Nach erfolgreicher Übertragung ZV-Begleitzettel ablegen:**
  Ist dieses Kontrollkästchen aktiviert, so wird zu jeder erfolgreich übertragenen Zahlungsverkehrsdatei ein Datenträger-Begleitzettel im PDF-Format abgelegt.

5.7. SRZ-Funktionen

Allgemeines

Die im folgenden Abschnitt beschriebenen Funktionen sind vor allem für Service-Rechenzentralen interessant.

Multivia Sm@rtConnect unterstützt die Erstellung von SEPA-XML-Containern inklusive Hashwerten. Zudem ist es möglich, den SRZ-Richtlinien entsprechende Datenträger-Begleitzettel zu erstellen.

Die SRZ-Funktionen finden Sie in einem eigenen Dialog, der unter dem Reiter "Zugänge" über die Schaltfläche "SRZ-Funktionen" aufgerufen werden kann. Dabei beziehen sich die vorgenommenen Einstellungen immer auf die ausgewählte Zugangs-ID.

Abbildung des Dialogs

In der folgenden Abbildung ist die Maske "SRZ-Einstellungen" abgebildet.

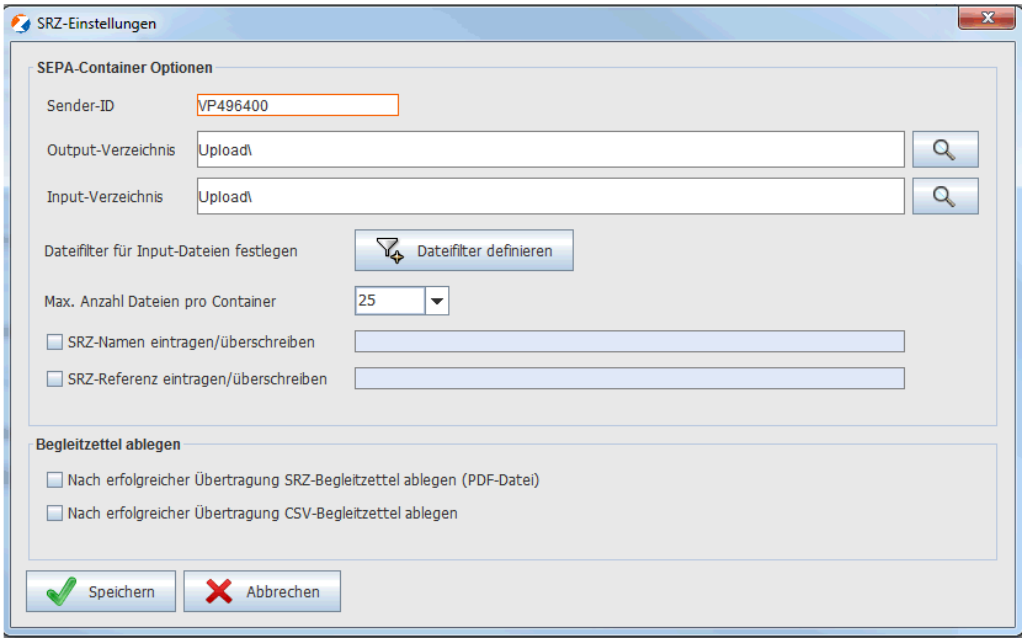


Abb. 5.14. SRZ-Einstellungen

Gruppierung "SEPA-Container-Optionen"

Die Einstellungen in dieser Gruppierung beziehen sich auf den Aufruf der Containererstellung im Konsolenmodus. Sie wirken sich nicht auf die Container-Erstellung mit Hilfe der Benutzeroberfläche aus.

- **Sender-ID:**
  Die Sender-ID ist die Identifikation des Datei-Absenders auf dem jeweiligen Zielsystem. Wenn die Datei über das EBICS-Verfahren übertragen wird, muss hier die EBICS-Kunden-ID eingetragen werden. Diese wird bei Anlage einer Zugangs-ID als Standard vorbelegt.

  Anmerkung
  Zusätzlich zu der Sender-ID wird von MVSC das Feld "Identification Type" mit dem Wert "EBIC" gefüllt. Dieser Wert gibt an, dass die angegebene Sender-ID aus dem EBICS-Verfahren stammt.

- **Output-Verzeichnis:**
  In dem hier angegebenen Verzeichnis werden die bei einem Konsolenaufruf erzeugten XML-Container abgelegt.
- **Input-Verzeichnis:**
  In diesem Verzeichnis werden Dateien gesucht, die zu einem XML-Container zusammengefasst werden. Die Input-Dateien müssen bestimmten Voraussetzungen entsprechen, damit sie zu einem Container zusammengefasst werden können. Näheres dazu finden Sie im Abschnitt "Voraussetzungen für die Container-Erstellung". Im Konsolenmodus werden nur Dateien berücksichtigt, die dem konfigurierten Dateifilter entsprechen.
- **Dateifilter für Input-Dateien festlegen:**
  Über die hier eingestellten Dateiendungen kann festgelegt werden, welche Dateitypen bei der Container-Erstellung berücksichtigt werden sollen. Der Dateifilter funktioniert nach dem gleichen Prinzip wie der Dialog "Vorbelegungen".
- **Max. Anzahl Dateien pro Container:**
  Über den hier angegebenen Wert kann festgelegt werden, ab welcher Anzahl von Dateien MVSC einen neuen XML-Container erstellen soll.

Anmerkung
Beachten Sie, dass schon bei wenigen Input-Dateien mehrere Container entstehen können. Dies hängt damit zusammen, dass bei der Container-Erstellung gewisse fachliche und technische Regeln berücksichtigt werden müssen, die es erforderlich machen, mehrere Container zu erstellen.

Ein Beispiel dafür ist die Trennung von Gutschriften und Lastschriften ("COR1", "CORE", "B2B").

- **SRZ-Namen eintragen/ überschreiben:**
  In den SEPA-Quelldateien, die zu einem Container zusammengefasst werden sollen, gibt es die Möglichkeit, den Namen des Datei-Einreichers (SRZ-Name) zu hinterlegen. Wenn der Name des Einreichers von dem dateierstellenden System nicht oder falsch belegt wurde, kann er mit MVSC nachträglich eingefügt bzw. überschrieben werden. Wird diese Option aktiviert, fügt MVSC den in dem Eingabefeld festgelegten SRZ-Namen in **alle** SEPA-Dateien ein, die dem Container hinzugefügt werden.

  Dabei wird pro Quelldatei die folgende fett markierte XML-Struktur eingefügt bzw. geändert:

  <GrpHdr>**<InitgPty><Nm>NAME DES SRZS</Nm></InitgPty>**</GrpHdr>
- **SRZ-Referenz eintragen/ überschreiben:**
  Genau wie der SRZ-Name kann die Referenz des Datei-Einreichers (SRZ-Referenz) in die SEPA-Quelldateien eingetragen werden. Falls das entsprechende Kontrollkästchen aktiviert wurde, wird die eingegebene SRZ-Referenz in **alle** SEPA-Quelldateien eingetragen, die dem Container hinzugefügt werden.

  In jede(r) Quelldatei wird dann die folgende XML-Struktur eingefügt/ geändert:

  <GrpHdr>**<InitgPty><Id><OrgId><Othr><Id>REFERENZ DES SRZS</Id></Othr></OrgId></Id></InitgPty>**</GrpHdr>

Gruppierung "Begleitzettel ablegen"

Die hier eingestellten Begleitzettel-Optionen haben sowohl in der Benutzeroberfläche als auch im Konsolenmodus Gültigkeit. Die Erstellung der Begleitzettel erfolgt nur dann, wenn die Daten erfolgreich übertragen wurden.

- **Nach erfolgreicher Übertragung SRZ-Begleitzettel ablegen (PDF-Datei):**
  Ist dieses Häkchen gesetzt, so wird parallel zu der übertragenen Datei ein SRZ-Begleitzettel abgelegt. Der SRZ-Begleitzettel enthält bei DTAUS-Formaten zusätzlich die in der Gruppe "DTAUS-Optionen" eingestellten Referenzdaten. Bei SEPA-Dateien wird der Begleitzettel mit dem in der Datei enthaltenen Hashwert ausgegeben. Außerdem werden die im GroupHeader enthaltenen Informationen (SRZ-Name/ SRZ-ID) mit ausgewiesen.
- **Nach erfolgreicher Übertragung CSV-Begleitzettel ablegen:**
  Wurde diese Option aktiviert, so werden die Begleitzettel-Informationen im CSV-Format (Comma Separated Values) abgelegt. Dabei wird pro logischer Einheit innerhalb der Auftragsdatei eine Zeile in der CSV-Datei erzeugt. Als Trennzeichen zwischen den einzelnen Werten wird das Semikolon verwendet. Die enthaltenen Informationen pro Zeile gleichen den Informationen, die auf den PDF-Begleitzetteln enthalten sind.

5.8. Container-Erstellung

Allgemeines

Mit Hilfe von MVSC können einzelne SEPA-XML-Dateien, die bestimmte Voraussetzungen erfüllen, zu einem XML-Containerformat zusammengefasst werden. Bei der Erstellung des Containersformats werden die einzelnen Eingangsdateien gemäß der SRZ-Richtlinien in das Containerformat eingebettet. Dafür werden die Eingangsdateien zunächst kanonisiert. Anschließend wird der sogenannte Hashwert (SHA-256) über die Dokumente gebildet. Der Hashwert dient als Kontrollmechanismus für die einzelnen Dokumente und ist deshalb auch auf dem Begleitzettel abgebildet.

Voraussetzungen für die Container-Erstellung

Damit einzelne SEPA-Dateien im pain-Format zu einem XML-Container zusammengefasst werden können, müssen die folgenden Voraussetzungen erfüllt sein:

- Die Eingangsdateien müssen in einem der folgenden pain-Formate vorliegen: Überweisungen: pain001, Lastschriften: pain008
- Die Dateien müssen gemäß dem zugrunde liegenden pain-Format korrekt aufgebaut sein (Prüfung gegen das XSD-Schema).
- Pro Datei darf nur ein Element vom Typ "Payment Information (<PmtInf>)" enthalten sein. Dieses Element kennzeichnet eine Zahlung, die aus verschiedenen Transaktionen bestehen kann.

Wenn der erstellte Container im Rahmen des SRZ-Verfahrens eingereicht werden soll, wird zudem empfohlen, die beiden Werte "Name des einreichenden Rechenzentrums" und "ID des einreichenden Rechenzentrums" im sogenannten "Group-Header" zu belegen.

Anmerkung
Die Belegung dieser Felder wird von MVSC nicht geprüft, daher können auch Container ohne diese Werte erstellt werden. Es ist jedoch möglich, diese Informationen nachträglich einzufügen oder zu ändern. Eine Beschreibung dazu finden Sie im Abschnitt "Gruppierung SEPA-Container-Optionen".

Container-Erstellung im Dialog

Die Container-Erstellung kann in der Benutzeroberfläche unter dem Reiter "Datenübertragung" über die Schaltfläche "Container erstellen" aufgerufen werden. Dabei wird das aktuell ausgewählte Verzeichnis als erstes Quellverzeichnis in den Dialog übernommen. Im oberen Bereich der Maske können auch andere Quellverzeichnisse ausgewählt werden. Auf der linken Seite wird der Inhalt (Dateien) des jeweils ausgewählten Quellverzeichnisses aufgelistet.

Die hier aufgelisteten Einträge können über die vorangestellten Kontrollkästchen selektiert und dem Container durch Betätigung der Schaltfläche mit dem Pfeil nach rechts hinzugefügt werden.

Sind alle gewünschten Dateien ausgewählt worden, so kann die Erstellung der Container über die Schaltfläche "Container erstellen" gestartet werden. Im folgenden Dialog müssen die Sender-ID und das Ausgabeverzeichnis angegeben werden. Die Angaben "SRZ-Name" und "SRZ-Referenz" sind dagegen optional.

Achtung
Bei der Erstellung von SEPA-XML-Containern werden die Eingangsdateien nach dem Pain-Format und nach dem Lastschriftverfahren (Basislastschrift oder Firmenlastschrift) getrennt. Dateien vom gleichen Typ werden dagegen bis zu der in den "SEPA-Container-Optionen" angegebenen Anzahl in demselben Container untergebracht.

Abbildung der Dialoge

In der folgenden Abbildung ist die Maske zur Dateiauswahl dargestellt:

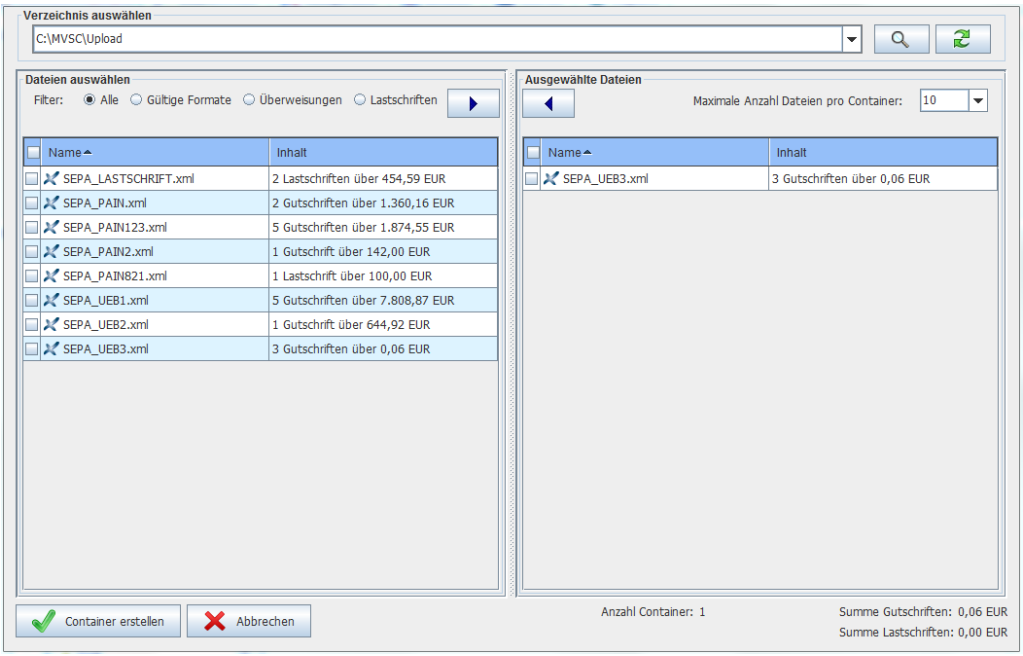


Abb. 5.15. Auswahl der Dateien für einen Container

In der folgenden Abbildung ist die Maske zur Containererstellung dargestellt:

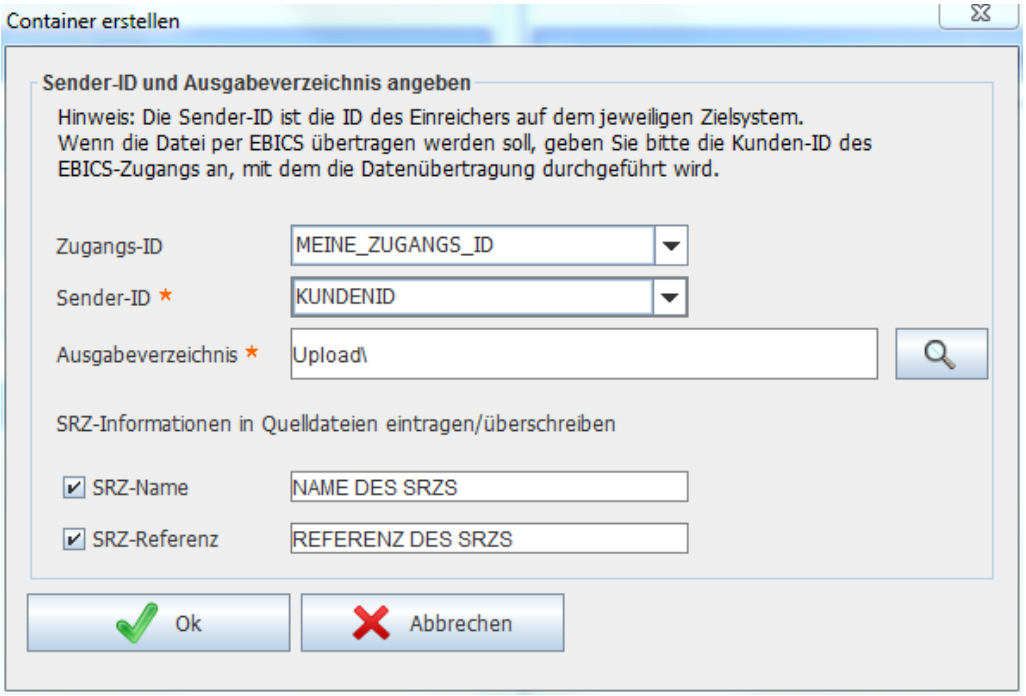


Abb. 5.16. Containererstellung

Hier müssen die Sender-ID und das Ausgabeverzeichnis angegeben werden.

Aufbau der Dateinamen

Die erstellten Containerdateien werden in dem angegebenen Ausgabeverzeichnis abgelegt. Der Aufbau der Dateinamen ist wie folgt strukturiert:

<Zeitstempel der Erstellung>_CONTAINERINHALT_SENDERID.SRZAUFTRAGSART

Beispiel Gutschriften:

20131130_162449_CONTAINER_GUTSCHRIFTEN_MEINEID1.CCS

Beispiel Lastschriften:

20131130_162449_CONTAINER_LASTSCHRIFTENCORE_MEINEID1.CDS

20131130_162449_CONTAINER_LASTSCHRIFTENB2B_MEINEID1.C2S

20131130_162449_CONTAINER_LASTSCHRIFTENCOR1_MEINEID1.C1S

Werden mehrere Dateien zum gleichen Zeitpunkt erstellt, so wird wie folgt noch ein Zähler ergänzt:

20131130_162449_CONTAINER_LASTSCHRIFTENCORE_MEINEID1_**1**.CDS

Container-Erstellung im Konsolenmodus

Die Container-Erstellung kann auch über die Kommandozeile aufgerufen werden. Wechseln Sie dafür wie folgt in das MVSC Installationsverzeichnis:

```
cd C:\Installations\Verzeichnis\MVSC\
```

Starten Sie die Container-Erstellung mit den gewünschten Parametern:

1. **Variante A: Es werden nur die Zugangs-ID und das Kennzeichen für die Container-Erstellung übergeben. Alle anderen Parameter werden aus der hinterlegten Konfiguration ermittelt. -jar**

   ```
   LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" "CONTAINER"
   ```

   Bei dieser Aufrufvariante werden die im Dialog "SRZ-Funktionen" hinterlegten Einstellungen verwendet. Dabei wird der eingestellte Dateifilter auf das angegebene Input-Verzeichnis angewendet. Die auf diese Art ermittelten Input-Dateien werden validiert und in das Container-Format eingebettet. Die erstellten Container werden im hinterlegten Ausgabeverzeichnis abgelegt.

   Anmerkung
   Die sogenannte "Sender-ID" und der Parameter "Maximale Anzahl Dateien pro Container" werden immer aus der Konfiguration ermittelt. Diese Werte können daher nicht über die Kommandozeile angegeben werden. Auch der Dateifilter muss vor dem Aufruf im Dialog "SRZ-Funktionen" konfiguriert werden.

2. **Variante B: Zugangs-ID, Container-Kennzeichen und Input-Verzeichnis werden übergeben.**

   ```
   LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" "CONTAINER"
    "Pfad/zum/Input/Verzeichnis"
   ```

   Dieser Aufruf unterscheidet sich nur in einem Punkt von Variante A:

   Das in der Konfiguration hinterlegte Input-Verzeichnis wird ignoriert. Stattdessen wird der übergebene Verzeichnispfad als Input-Verzeichnis verwendet. Alle weiteren Parameter werden aus der Konfiguration ermittelt.

3. **Variante C: Zugangs-ID, Container-Kennzeichen sowie Input- und Output-Verzeichnis werden angegeben.**

   ```
   LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" "CONTAINER"
    "Pfad/zum/Input/Verzeichnis" "Pfad/zum/Output/Verzeichnis"
   ```

   Wie in Variante B wird hier das Input-Verzeichnis übergeben. Bei diesem Aufruf wird jedoch zusätzlich das Output-Verzeichnis angegeben. Dieses wird statt des in der Konfiguration gespeicherten Output-Verzeichnisses verwendet.

Rückgabewerte und Fehlerbehandlung

MVSC prüft, ob Dateien, die einem Container hinzugefügt werden sollen, grundsätzlich für Containerformate geeignet sind. Dabei wird geprüft, ob die unter "Voraussetzungen" beschriebenen Bedingungen erfüllt sind.

Ist dies nicht der Fall, so wird in der Benutzeroberfläche ein entsprechender Hinweis ausgegeben. Die Datei wird nicht in den Container aufgenommen.

Passiert dies dagegen im Konsolenmodus, so wird die Container-Erstellung abgebrochen: Es wird kein Container erstellt und das Programm gibt einen entsprechenden Rückgabewert zurück.

Die möglichen Rückgabewerte des Konsolenmodus sind in der folgenden Tabelle aufgelistet:

Rückgabewert	Bedeutung
-1	Die EBICS-Zugangsdaten sind unvollständig oder fehlerhaft.
-4	Es wurde keine Input-Dateien gefunden (gemäß Dateifilter und Input-Verzeichnis).
-6	Parameterfehler: Die Aufrufparameter sind nicht korrekt.
-8	Mindestens ein Verzeichnis konnte nicht gefunden werden (Validierung der Input/Output-Verzeichnisse).
-9	Doppelaufruf: Die Anwendung wurde bereits gestartet.
1	**Die Container-Erstellung war erfolgreich, es wurde mindestens ein Container erstellt.**
31	Das Dateiformat mindestens einer Input-Datei ist unbekannt.
32	XML-Format ungültig: Eine Datei entspricht nicht den für Containern zugelassenen SEPA-Formaten.
33	XML-Validierung fehlgeschlagen: Eine Datei enthält Formatfehler gemäß dem XML-Schema.
34	XML-Validierung: Es ist mehr als ein <PmtInf>-Block in der Datei enthalten (mehrere logische Dateien).
35	XML-Validierung: Der Service-Level ist für Container ungültig.
36	XML-Validierung: Das Local-Instrument ist für Container ungültig.
37	XML-Erstellung: Es ist ein Fehler bei der Kanonisierung einer Input-Datei aufgetreten.
38	XML-Erstellung: Es ist ein Fehler bei der Hashwert-Berechnung aufgetreten.
39	XML-Erstellung: Es ist ein technischer Fehler beim Schreiben einer Container-Datei aufgetreten.

Generell weisen die negativen Rückgabewerte auf Konfigurations- bzw. Aufruf-Probleme hin, während die Werte im 30'er Bereich entweder auf Fehler in den Input-Dateien (31 bis 36) oder Fehler beim Schreiben der Containerdateien zurückzuführen sind.

Container erstellen

Mit Hilfe der verschiedenen Aufrufvarianten im Konsolenmodus kann die Container-Erstellung mit dem Dateiversand kombiniert werden. Dafür reichen bereits die von MVSC als Standard verwendeten Einstellungen.

Die folgenden Vorbedingungen müssen erfüllt sein:

- Die Aufrufe müssen mit einer vollständig initialisierten Zugangs-ID (inklusive der Abholung der Auftragsarten) durchgeführt werden.
- Im Dialog "SRZ-Funktionen" müssen ggf. das Input-Verzeichnis und der Dateifilter an Ihr System/ Ihre Input-Dateien angepasst werden.
- In dem angegebenen Input-Verzeichnis müssen sich Dateien befinden, die dem eingestellten Dateifilter (Standard ist "XML") entsprechen. Informationen zu den weiteren Voraussetzungen für die Containererstellung finden Sie im Abschnitt "Voraussetzungen für die Container-Erstellung".
- Als Output-Verzeichnis für die Container wurde das Upload-Verzeichnis der Zugangs-ID angegeben (Standard).

Wechseln Sie in das MVSC-Verzeichnis und führen Sie einen der im Abschnitt "Container-Erstellung im Konsolenmodus" beschriebenen Aufrufe durch.

```
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" "CONTAINER"
```

Wenn der Aufruf erfolgreich verlief (Rückgabewert 1), wurde mindestens eine Container-Datei in das Output-Verzeichnis eingestellt. Den Aufbau der Dateinamen der erstellten Container-Dateien finden Sie im Abschnitt "Aufbau der Dateinamen". Die Dateinamen enden immer mit der benötigten EBICS-Auftragsart.

Container versenden

Zum Versenden des Containers wird folgender Aufruf verwendet:

```
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" "Auftragsart"
```

Falls aus Ihren Input-Dateien verschiedene Container-Typen erstellt werden, müssen Sie die Datenübertragung mit den verschiedenen Auftragsarten starten, damit alle Dateien übertragen werden.

```
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" CCS
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" CDS
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" C1S
LibJAV\bin\java -Xms96m -Xmx256m -jar "MVSC.jar" "MEINE_ZUGANGS_ID" C2S
```

Bei diesen Aufrufen werden alle Dateien aus dem Upload-Verzeichnis übertragen, die dem für die übergebene Auftragsart konfigurierten Dateifilter entsprechen.

Als Standard hinterlegt MVSC die Kennung der Auftragsart in den einzelnen Dateifiltern. Dadurch passen die erstellten Container-Dateien zu den Dateifiltern der jeweiligen Auftragsart.

5.9. Empfängerprüfung (Verification of Payee ["VoP"])

Voraussetzungen

Seit dem Oktober 2025 gelten Vorgaben für SEPA-Überweisungen und für SEPA-Echtzeitüberweisungen, die beinhalten, dass die Möglichkeit bestehen muss, die Angaben zum Zahlungsempfänger mit den bei der Bank zur angegebenen IBAN gespeicherten Empfängerdaten abzugleichen.

Um diese Empfängerprüfung (**V**erification **o**f **P**ayee; im Folgenden auch "VoP" genannt) in MVSC nutzen zu können, sind für den Teilnehmer die im Folgenden beschriebenen neuen Opt-In-Auftragsarten (d.h. Auftragsarten mit Empfängerprüfung) erforderlich:

Auftragsarten für die Einreichung: "CIV" (Sammler mit SEPA-Echtzeitüberweisungen mit VoP), "CTV" (SEPA-Überweisung mit VoP)

Diese sind in der folgenden Abbildung beispielhaft dargestellt:

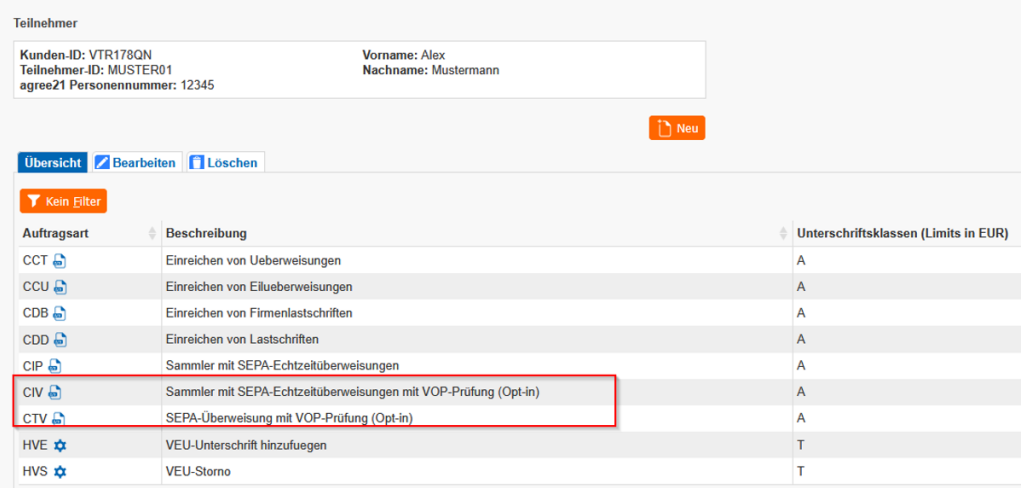


Abb. 5.17. VoP: Auftragsarten zur Einreichung

Auftragsart für die Abholung: "VPZ" (VoP Statusreport)

Diese ist in der folgenden Abbildung beispielhaft dargestellt:

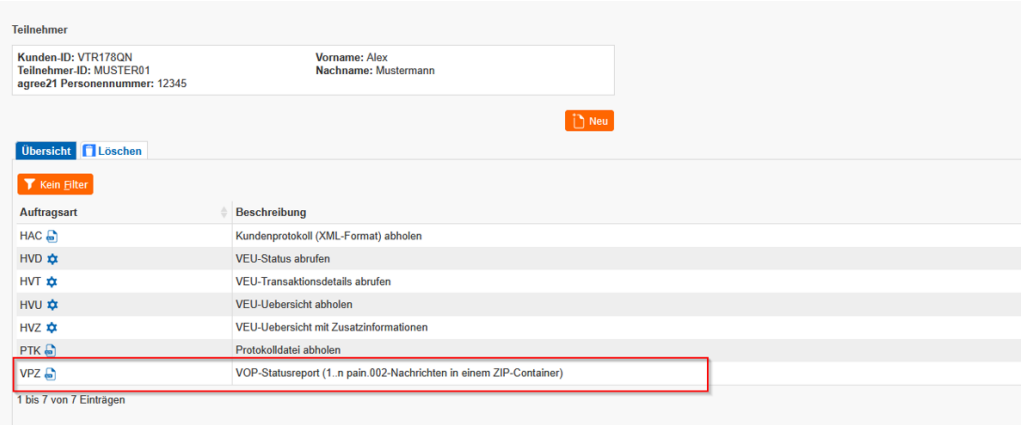


Abb. 5.18. VoP: Auftragsart zur Abholung

Sie können diese Auftragsarten vom Bankrechner abholen und in Ihre MVSC-Datenbank einpflegen. Die Vorgehensweise der Abholung dieser Auftragsarten ist abhängig von der von Ihnen verwendeten EBICS-Version:

Unter der **EBICS-Version 2.5** können Sie die Auftragsarten nach Aufruf des Reiters "Zugänge" über die gleichnamige Schaltfläche "Berechtigungen abrufen" abrufen. Diese Schaltfläche ist in der folgenden Abbildung im unteren Bereich der Maske rot markiert dargestellt:

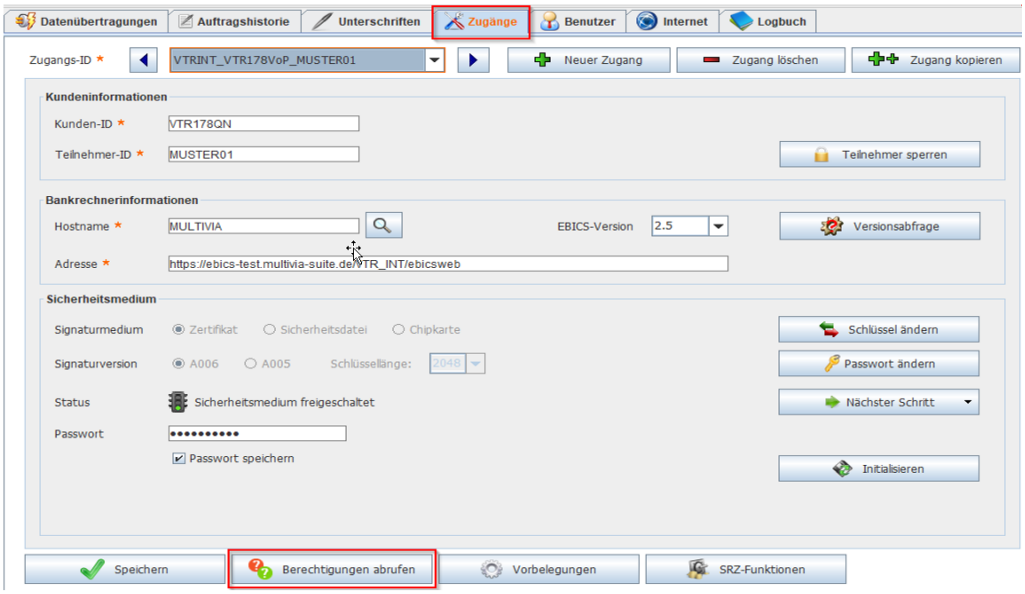


Abb. 5.19. VoP: Berechtigungen abrufen

Unter der **EBICS-Version 3.0** erfolgt der Abruf der Auftragsarten ebenfalls über den Reiter "Zugänge",- hier ist aber die Schaltfläche "Service abrufen" zu verwenden. Diese ist in der folgenden Abbildung im unteren Bereich der Maske rot markiert dargestellt:

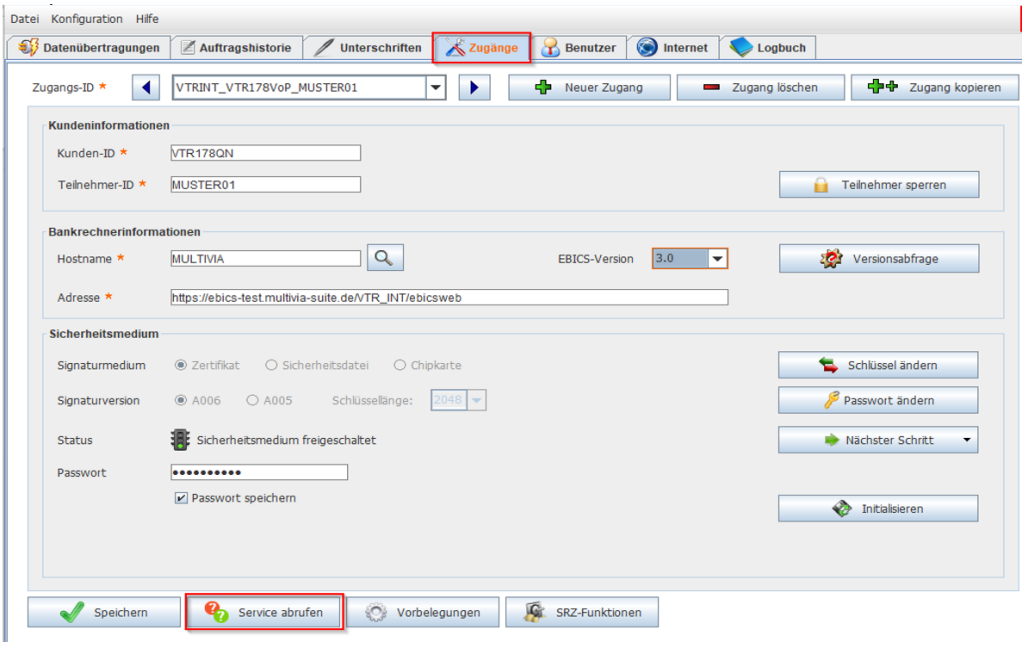


Abb. 5.20. VoP: Service abrufen

Nach Abruf der Auftragsarten vom Bankrechner sind diese wie in der folgenden Abbildung dargestellt in der MVSC-Datenbank eingepflegt.

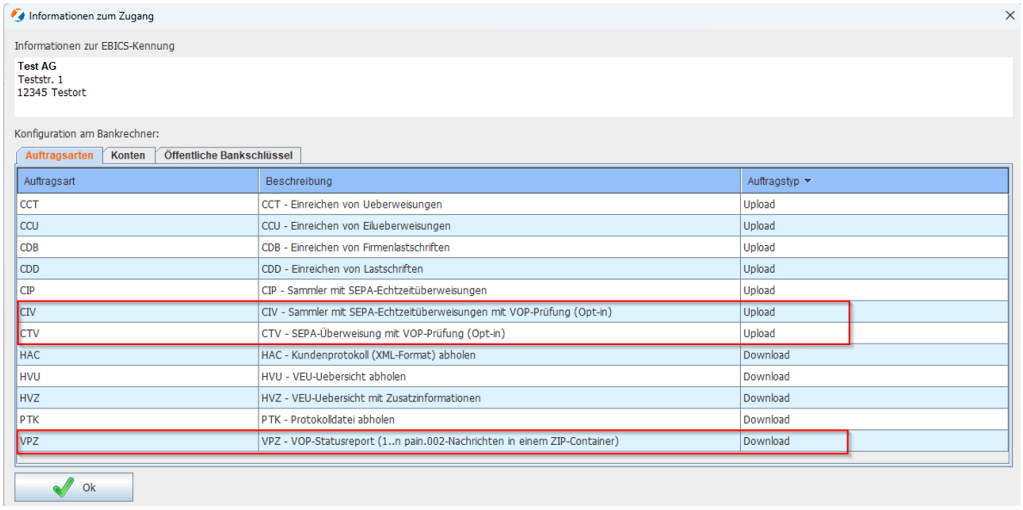


Abb. 5.21. VoP: Ergebnis des Abrufs der Auftragsarten

Vorbelegungen

Sie können spezifische Vorbelegungen für die Empfängerprüfung ("VoP") vornehmen. Wählen Sie dafür unter dem Reiter "Zugänge" die Schaltfläche "Vorbelegungen" im unteren Bereich der Maske.

Diese Schaltfläche ist in der folgenden Abbildung im unteren Bereich rot markiert dargestellt:

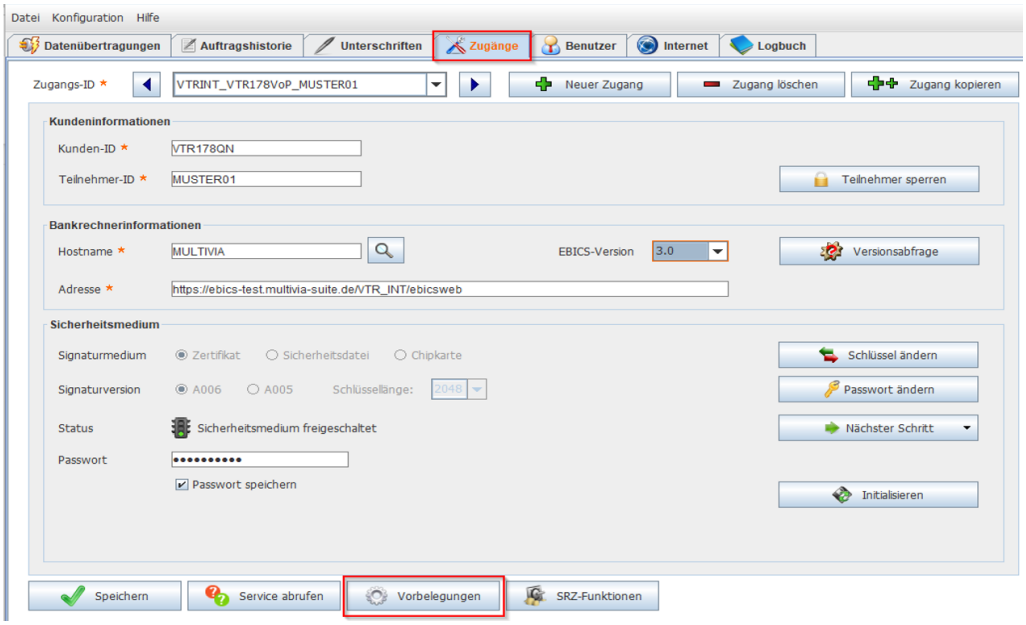


Abb. 5.22. VoP: Vorbelegungen aufrufen

Sie erhalten dann die in der folgenden Abbildung dargestellte Maske:

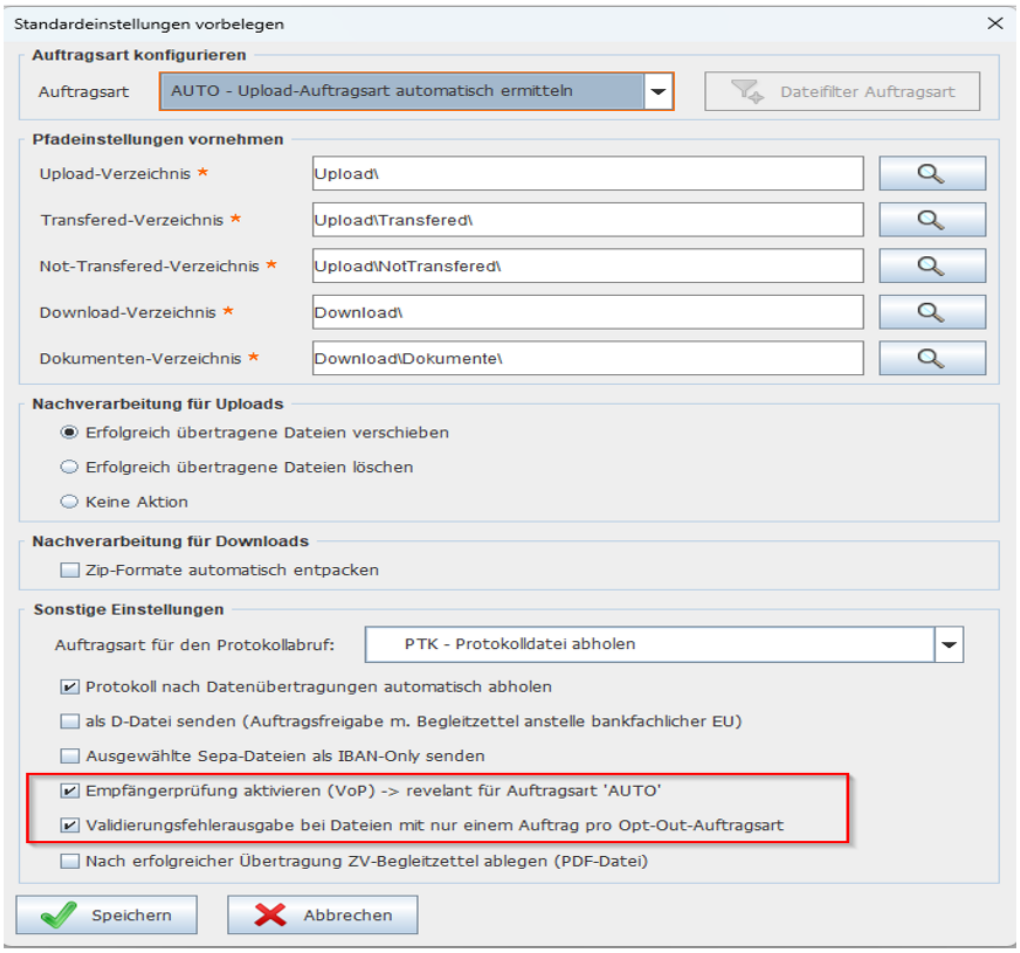


Abb. 5.23. VoP: Vorbelegungen vornehmen

Hier finden Sie im unteren Bereich der abgebildeten Maske die beiden rot markierten Kontrollkästchen

- "Empfängerprüfung aktivieren (VoP) -> relevant für Auftragsart 'AUTO' "

und

- "Validierungsfehlerausgabe bei Dateien mit nur einem Auftrag pro Opt-Out-Auftragsart" (d.h. ohne Empfängerprüfung).

Über das **Kontrollkästchen "Empfängerprüfung aktivieren (VoP)"** können Sie die Empfängerprüfung für die Auftragsart "AUTO" aktivieren oder deaktivieren.

Bei Aktivierung bedeutet das, dass für diesen Zugang bei Auswahl der Auftragsart "AUTO" in der Datenübertragung die Opt-In-Auftragsarten (d.h. Auftragsarten mit Empfängerprüfung,- z.B. "CTV", "CIV") verwendet werden.

Über das **Kontrollkästchen "Validierungsfehlerausgabe bei Dateien mit nur einem Auftrag pro Opt-Out-Auftragsart"** können Sie steuern, ob eine Fehlermeldung erzeugt werden soll, sofern eine Datenübertragung mit einer Opt-Out-Auftragsart (d.h. ohne Empfängerprüfung) erfolgt, bei der die zu übertragende Datei nur einen Auftrag enthält. Nur wenn die Checkbox aktiviert ist wird eine solche Fehlermeldung ausgegeben. Ein automatischer Wechsel zu einer Opt-In-Auftragsart erfolgt nicht.

Datenübertragung mit oder ohne Empfängerprüfung in der Benutzeroberfläche (GUI / Graphical User Interface)

Es ist zunächst zu prüfen, dass die beiden im obigen Abschnitt "Vorbelegungen" beschriebenen Kontrollkästchen

- Empfängerprüfung aktivieren (VoP) -> relevant für Auftragsart 'AUTO'

und

- Validierungsfehlerausgabe bei Dateien mit nur einem Auftrag pro Opt-Out-Auftragsart

korrekt gepflegt sind.

Bei der Datenübertragung sind dann keine weiteren Angaben erforderlich.

Datenübertragung mit "VoP" (Opt-In-Auftragsart, d.h. mit Empfängerprüfung) bei der Auftragsart "AUTO":

Voraussetzung: Der Zugang enthält bei den Vorbelegungen **die Aktivierung** der Checkbox "Empfängerprüfung aktivieren (VoP)".

Bei der Datenübertragung wird die Auftragsart "AUTO" ausgewählt.

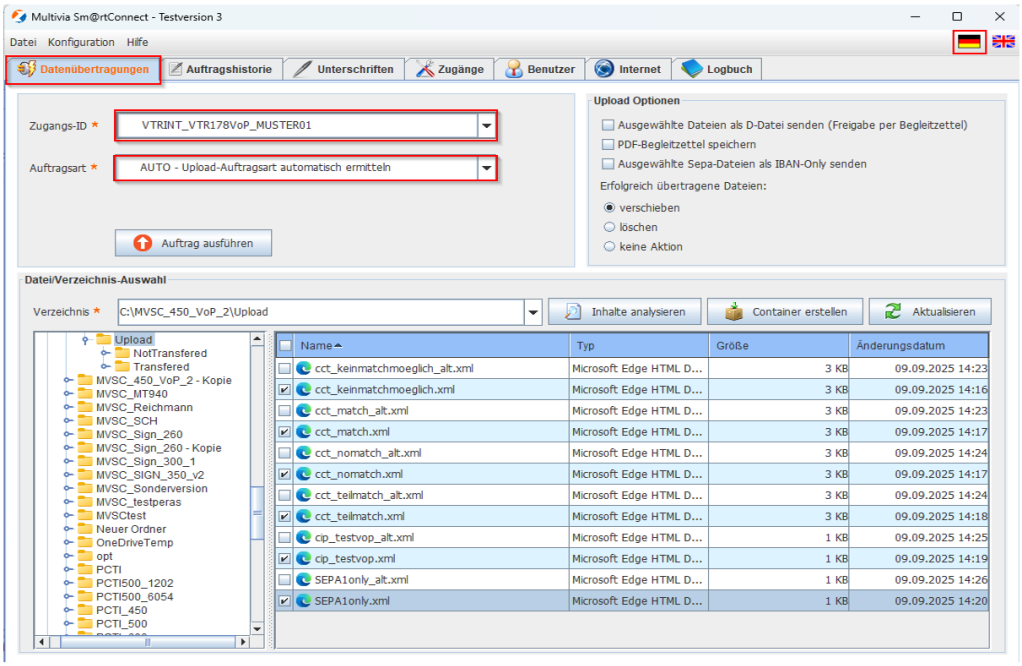


Abb. 5.24. VoP: Datenübertragung mit der Auftragsart "AUTO"

Der Anwender wählt die zu übertragenen Dateien aus. Anschließend nutzt er die Schaltfläche "Auftrag ausführen".

Die Auftragsarten werden dann automatisch zugewiesen und die Dateien werden übertragen.

Das Ergebnis ist in der folgenden Abbildung beispielhaft dargestellt:

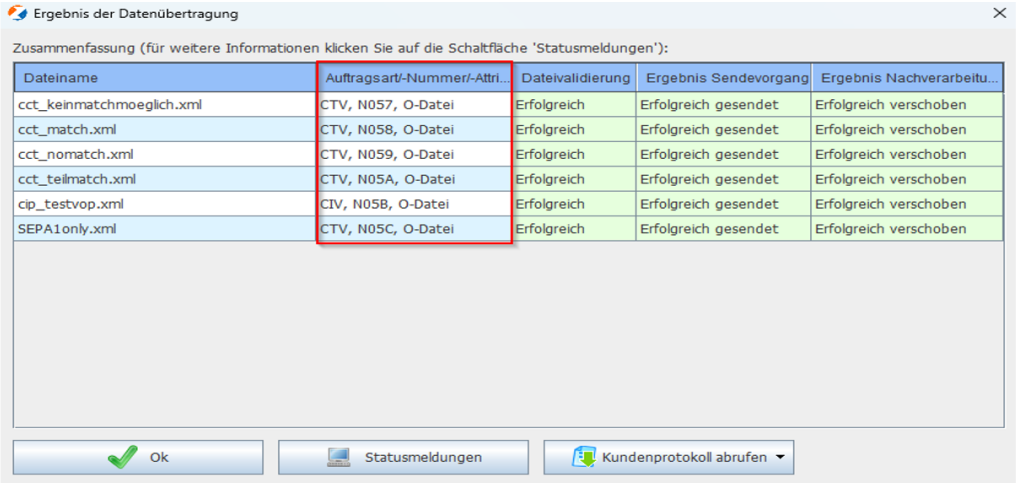


Abb. 5.25. VoP: Ergebnis der Datenübertragung mit der Auftragart "AUTO"

In diesem Fall werden automatisch nur die Opt-in-Auftragsarten verwendet.

Datenübertragung ohne "VoP" (Opt-Out-Auftragsart, d.h ohne Empfängerprüfung) bei der Auftragsart "AUTO":

Voraussetzung: Der Zugang enthält bei den Vorbelegungen **die Deaktivierung** der Checkbox "Empfängerprüfung aktivieren (VoP)".

Bei der Datenübertragung wird wie in der folgenden Abbildung dargestellt die Auftragsart "AUTO" ausgewählt.

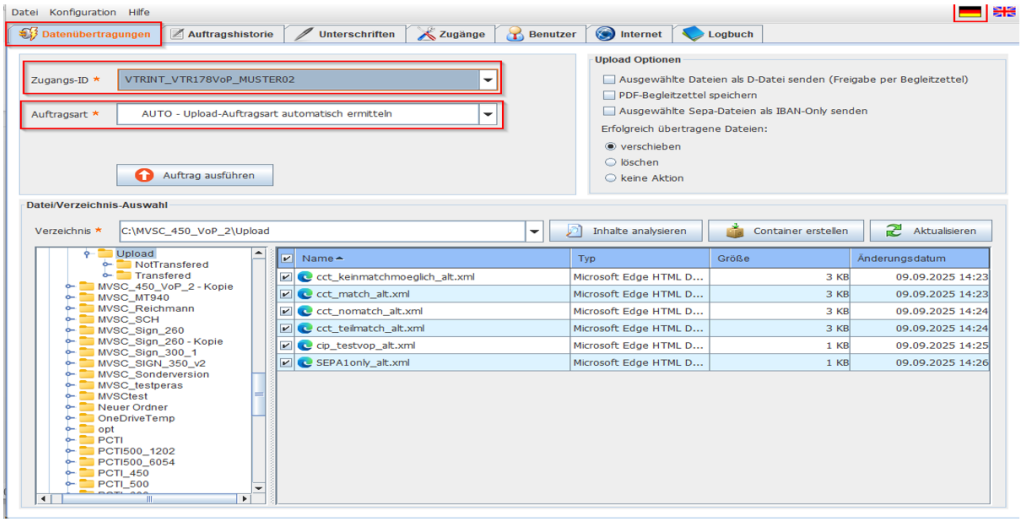


Abb. 5.26. VoP: Datenübertragung mit der Auftragsart "AUTO"

Der Anwender wählt die zu übertragenen Dateien aus und nutzt anschließend die Schaltfläche "Auftrag ausführen".

Die Auftragsarten werden automatisch zugewiesen und die Dateien werden übertragen.

Das Ergebnis ist in der folgenden Abbildung beispielhaft dargestellt:

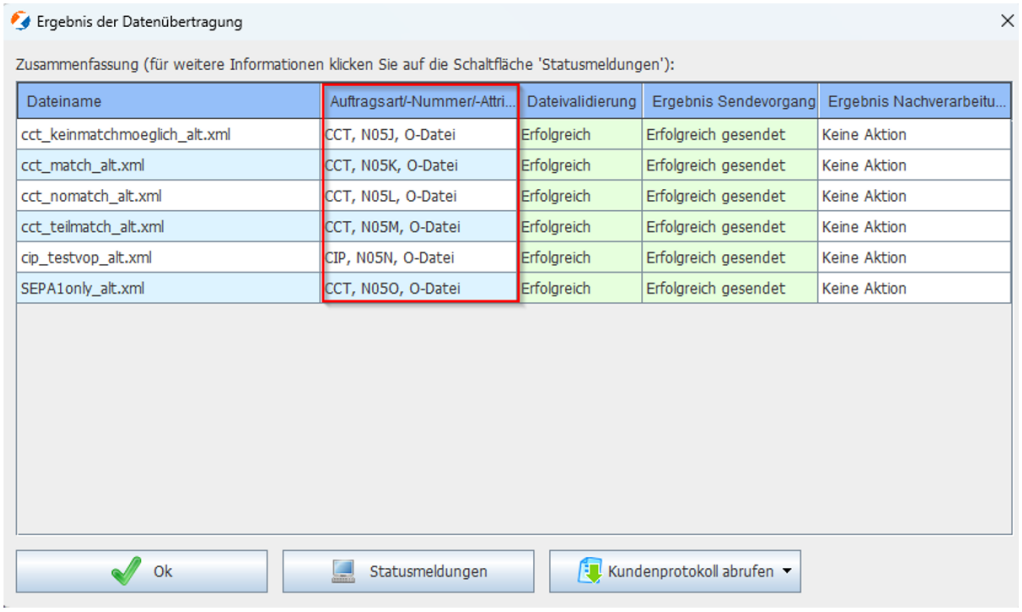


Abb. 5.27. VoP: Ergebnis der Datenübertragung mit der Auftragart "AUTO"

Es werden in diesem Fall automatisch nur die Opt-Out-Auftragsarten verwendet.

Datenübertragung mit allen anderen Auftragsarten außer der Auftragsart "AUTO":

Es kann auch gezielt eine Auftragsart aus der Auftragsartenliste ausgewählt werden. Diese wird dann unabhängig davon, ob es eine Opt-in oder eine Opt-out-Auftragsart ist, verwendet.

Dies ist in der folgenden Abbildung beispielhaft dargestellt:

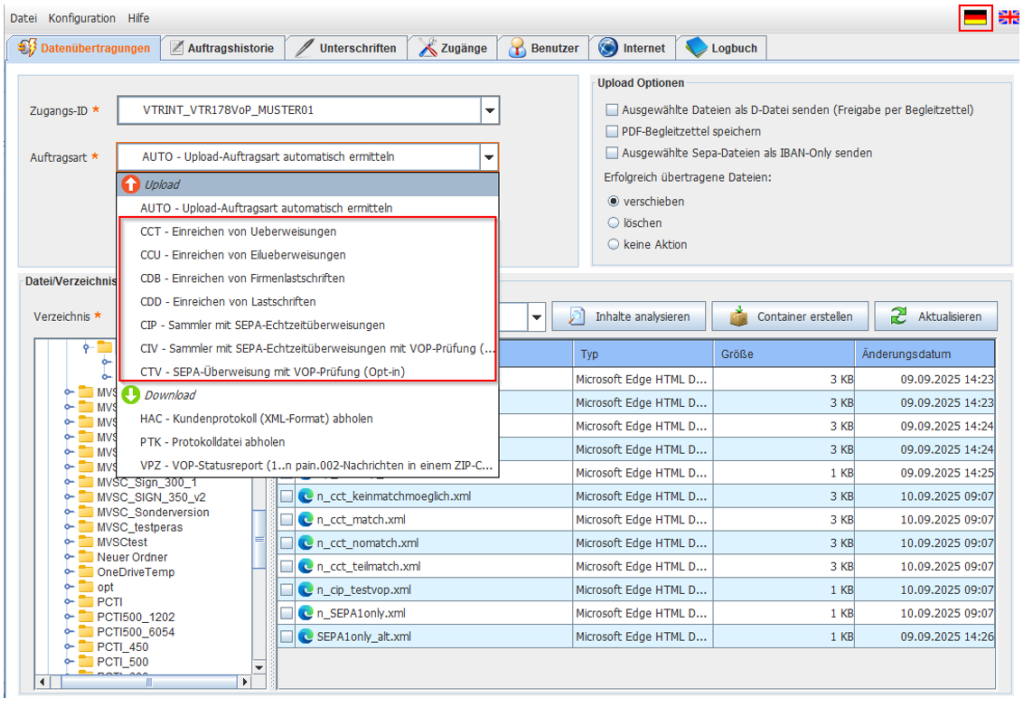


Abb. 5.28. VoP: Datenübertragung mit anderer Auftragart als "AUTO"

In der folgenden Tabelle sind die jeweiligen Opt-Out- und Opt-In-Auftragsarten dargestellt:

Opt-Out-Auftragsart (d.h. ohne Empfänger-prüfung)	Opt-In-Auftragsart (d.h. mit Empfängerprü-fung)
CCT	CTV

Opt-Out-Auftragsart (d.h. ohne Empfängerprüfung)	Opt-In-Auftragsart (d.h. mit Empfängerprüfung)
XCT	XTV
CIP	CIV
CCU	-
XCU	-
CCC	-
XCC	-
XCI	-
CCS	VCS
CIS	VIS
CCX	VCX
CIX	VIX

Angaben zur Datenübertragung mit oder ohne Empfängerprüfung im Batch-Modus (automatischer Modus)

Es ist auch hier zunächst zu überprüfen, dass die beiden im obigen Abschnitt "Vorbelegungen" beschriebenen Kontrollkästchen

- "Empfängerprüfung aktivieren (VoP)"

und

- "Validierungsfehlerausgabe bei Dateien mit nur einem Auftrag pro Opt-Out-Auftragsart"

korrekt gepflegt sind.

Datenübertragung mit VoP (Opt-In-Auftragsarten) mit der Auftragsart "AUTO"

Bei der Batch-Datenübertragung im Batch-Job müssen keine Anpassungen vorgenommen werden, sofern die Auftragsart "AUTO" verwendet wird.

In den Vorbelegungen der einzelnen Zugänge ist hinterlegt, ob mit Opt-In-Auftragsarten oder mit Opt-Out-Auftragsarten übertragen werden soll. Diese Eintragungen werden berücksichtigt.

Aufruf mit der Auftragsart "AUTO":

```
java -jar "MVSC.jar" <$MEINE_ZUGANGSID> AUTO <$MEIN_UPLOADVERZEICHNIS>
```

Datenübertragung mit allen anderen Auftragsarten außer der Auftragsart "AUTO"

Werden allerdings qualifizierte Opt-Out-Auftragsarten im Aufruf des Batch-Jobs genutzt, so können Sie diese, falls gewünscht, durch Opt-In-Auftragsarten ersetzen.

Beispiel:

Wird beispielsweise die vorherige Nutzung der Opt-Out-Auftragsart "CCT" ersetzt durch die Verwendung der Opt-In Auftragsart "CTV", so sieht der Aufruf wie folgt aus:

Vorheriger Aufruf mit der Opt-Out-Auftragsart "CCT":

```
java -jar "MVSC.jar" <$MEINE_ZUGANGSID> CCT <$MEIN_UPLOADVERZEICHNIS>
```

Neuer Aufruf mit der Opt-In-Auftragsart "CTV":

```
java -jar "MVSC.jar" <$MEINE_ZUGANGSID> CTV <$MEIN_UPLOADVERZEICHNIS>
```

Weiterverarbeitung der Aufträge in der VEU

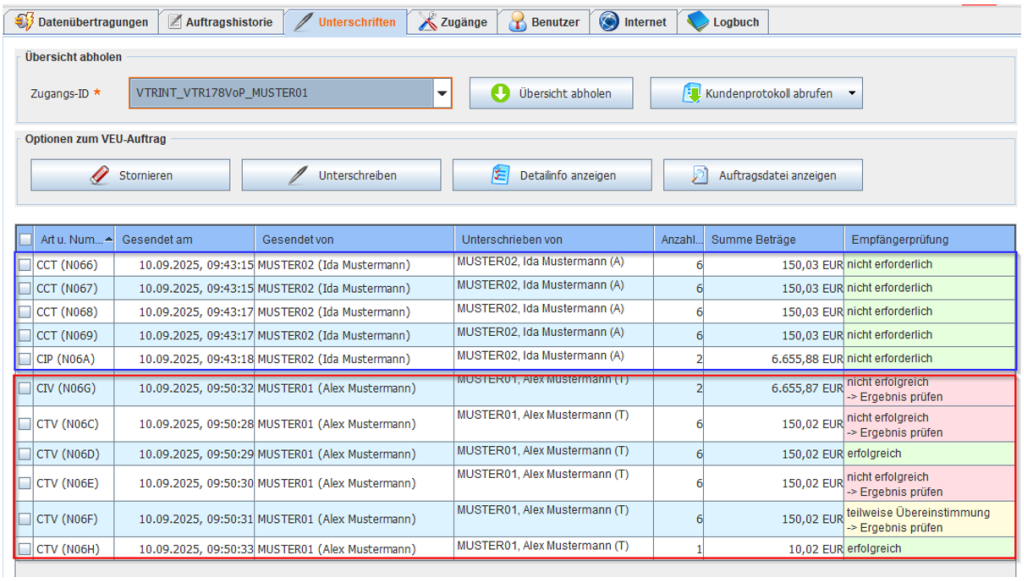
Beachten Sie die folgende wichtige Information:

Achtung

Alle Zahlungsverkehrsdateien, die mit Empfängerprüfung (d.h. mit einer Opt-In-Auftragsart wie beispielsweise "CTV") übertragen werden, werden grundsätzlich **nur mit Transportunterschrift** in die VEU eingestellt. Diese müssen somit noch unterschrieben werden!

In der Unterschriftenübersicht werden alle zu unterschreibenden Dateien aufgeführt.

Diese Unterschriftenübersicht ist in der folgenden Abbildung beispielhaft dargestellt:



Art u. Num...	Gesendet am	Gesendet von	Unterschrieben von	Anzahl...	Summe Beträge	Empfängerprüfung
CCT (N066)	10.09.2025, 09:43:15	MUSTER02 (Ida Mustermann)	MUSTER02, Ida Mustermann (A)	6	150,03 EUR	nicht erforderlich
CCT (N067)	10.09.2025, 09:43:15	MUSTER02 (Ida Mustermann)	MUSTER02, Ida Mustermann (A)	6	150,03 EUR	nicht erforderlich
CCT (N068)	10.09.2025, 09:43:17	MUSTER02 (Ida Mustermann)	MUSTER02, Ida Mustermann (A)	6	150,03 EUR	nicht erforderlich
CCT (N069)	10.09.2025, 09:43:17	MUSTER02 (Ida Mustermann)	MUSTER02, Ida Mustermann (A)	6	150,03 EUR	nicht erforderlich
CIP (N06A)	10.09.2025, 09:43:18	MUSTER02 (Ida Mustermann)	MUSTER02, Ida Mustermann (A)	2	6.655,88 EUR	nicht erforderlich
CIV (N06G)	10.09.2025, 09:50:32	MUSTER01 (Alex Mustermann)	MUSTER01, Alex Mustermann (T)	2	6.655,87 EUR	nicht erfolgreich -> Ergebnis prüfen
CTV (N06C)	10.09.2025, 09:50:28	MUSTER01 (Alex Mustermann)	MUSTER01, Alex Mustermann (T)	6	150,02 EUR	nicht erfolgreich -> Ergebnis prüfen
CTV (N06D)	10.09.2025, 09:50:29	MUSTER01 (Alex Mustermann)	MUSTER01, Alex Mustermann (T)	6	150,02 EUR	erfolgreich
CTV (N06E)	10.09.2025, 09:50:30	MUSTER01 (Alex Mustermann)	MUSTER01, Alex Mustermann (T)	6	150,02 EUR	nicht erfolgreich -> Ergebnis prüfen
CTV (N06F)	10.09.2025, 09:50:31	MUSTER01 (Alex Mustermann)	MUSTER01, Alex Mustermann (T)	6	150,02 EUR	teilweise Übereinstimmung -> Ergebnis prüfen
CTV (N06H)	10.09.2025, 09:50:33	MUSTER01 (Alex Mustermann)	MUSTER01, Alex Mustermann (T)	1	10,02 EUR	erfolgreich

Abb. 5.29. VoP: Unterschriften

In der Abbildung der Tabelle sehen Sie im oberen Bereich der ersten fünf Tabellenzeilen, der blau umrahmt ist, die Opt-Out-Auftragsarten "CCT" und "CIP". Für diese werden keine Empfängerprüfungen vorgenommen. Daher steht in der rechten Spalte mit der Überschrift "Empfängerprüfung" nur "nicht erforderlich".

Hier ist keine Überprüfung durch den Anwender erforderlich.

Im unteren Bereich der letzten sechs Tabellenzeilen, die rot umrahmt sind, sehen Sie dagegen die Opt-In-Auftragsarten. Für diese ist in der ganz rechten Spalte mit der Überschrift "Empfängerprüfung" jeweils ein Status der Empfängerprüfung eingetragen.

Hierfür gibt es drei mögliche Status:

1. erfolgreich (mit grünem Hintergrund)
2. teilweise Übereinstimmung (mit gelbem Hintergrund)
3. nicht erfolgreich (mit rotem Hintergrund)

Detailinformationen zu den einzelnen Dateien können durch "Doppelklick" auf die jeweilige Zeile der Tabelle aufgerufen werden.

In der folgenden Abbildung ist beispielhaft eine solche Detailinformation zu sehen:

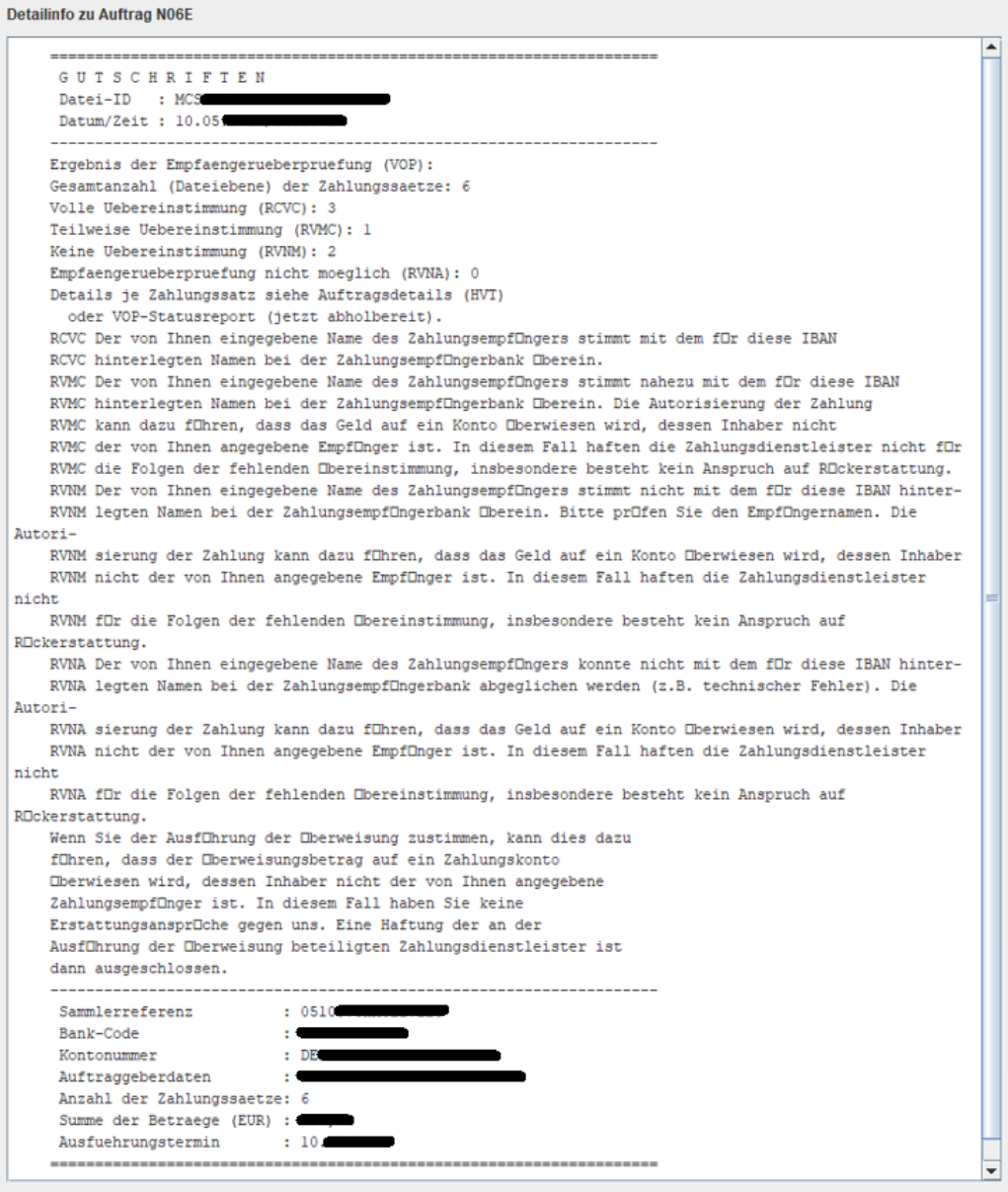


Abb. 5.30. VoP: Detailinformation zu einzelnen Übertragungen in der VEU

Näheres zur Leistung einer Unterschrift finden Sie im Kapitel "Datenübertragung im Dialog", Unterkapitel "Verteilte elektronische Unterschrift".

Statusreport abholen und Statusdatei einsehen

Möchten Sie nähere Informationen zur Empfängerprüfung ("VoP") einzelner Dateien erhalten, so haben Sie die Möglichkeit, den Statusreport zur Empfängerprüfung vom Bankrechner abzuholen und einzusehen.

Statusreport abholen

Um den Statusreport abzuholen wählen Sie unter dem Reiter "Datenübertragung" die Download-Auftragsart "VPZ" aus und gehen Sie auf "Auftrag ausführen".

Dies ist in der folgenden Abbildung dargestellt:

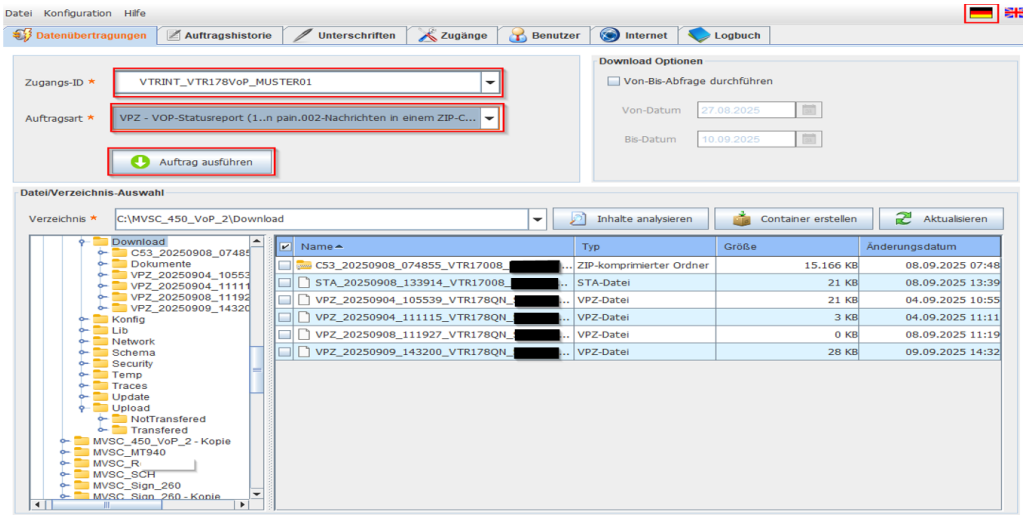


Abb. 5.31. VoP: Statusreport abholen, Schritt 1

Im folgenden Schritt bestätigen Sie die Frage, ob die im ZIP-Format empfangenen Daten entpackt werden sollen, wie in der folgenden Abbildung dargestellt mit "Ja".

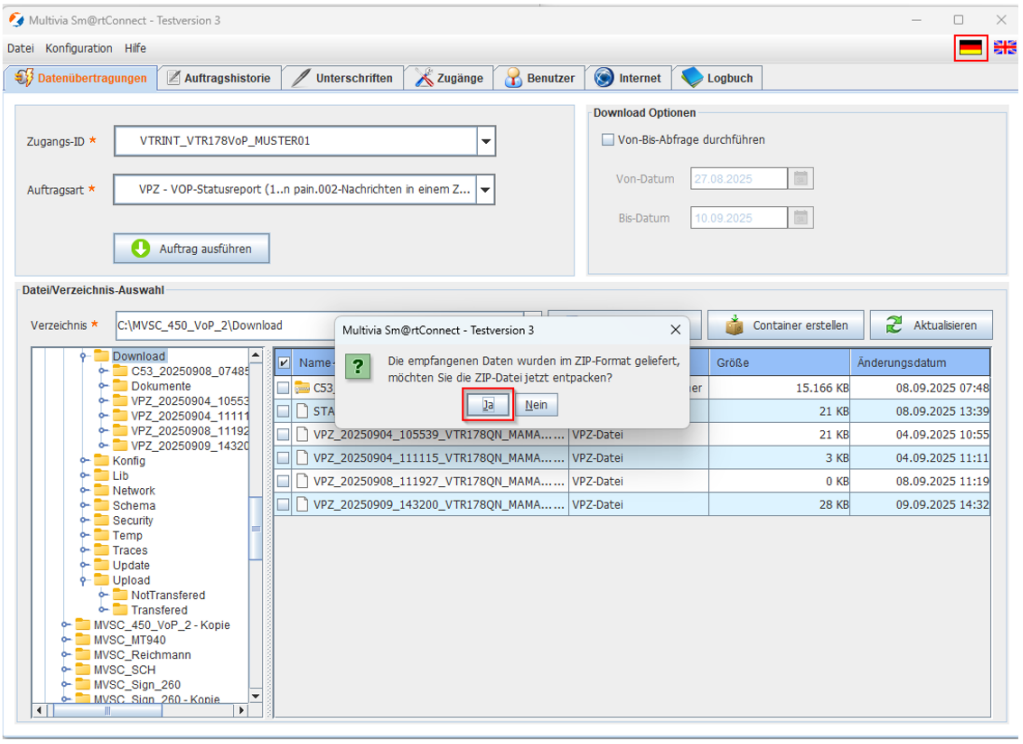


Abb. 5.32. VoP: Statusreport abholen, Schritt 2

Die Statusprotokolle werden dann in einer Liste aufgeführt.

In der folgenden Abbildung ist beispielhaft eine solche Liste von Statusprotokollen dargestellt:

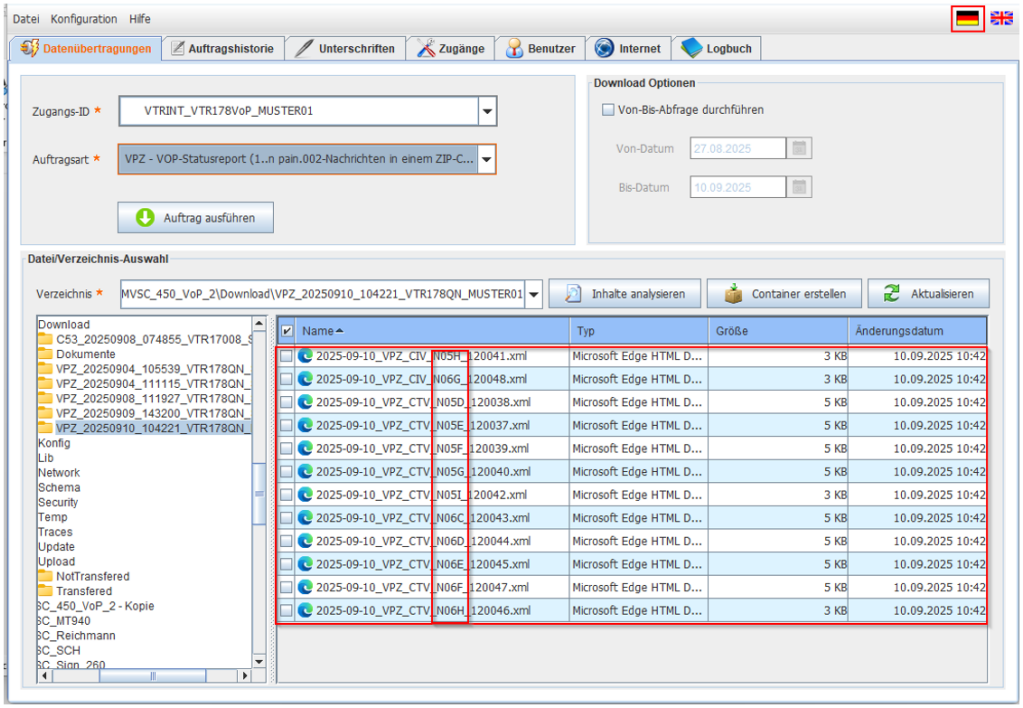


Abb. 5.33. VoP: Statusprotokolle

Dateien **der Atruvia** können anhand der Auftragsnummer identifiziert werden. Die Auftragsnummer finden Sie für Aufträge **der Atruvia** in der Spalte "Name" im Namen hinter der Auftragsart. In der oberen Abbildung ist die Auftragsnummer rot gekennzeichnet.

Beispiel: Der Name der Auftragsdatei lautet "2025-09-10_VPZ_CIV_**N05H**_20041.xml". Die Auftragsnummer lautet "N05H".

Anzeige der VoP-Statusdatei

Die VoP-Statusdatei kann nun angezeigt und als PDF-Dokument gespeichert oder ausgedruckt werden.

In der folgenden Abbildung ist beispielhaft die Anzeige einer Statusdatei abgebildet:

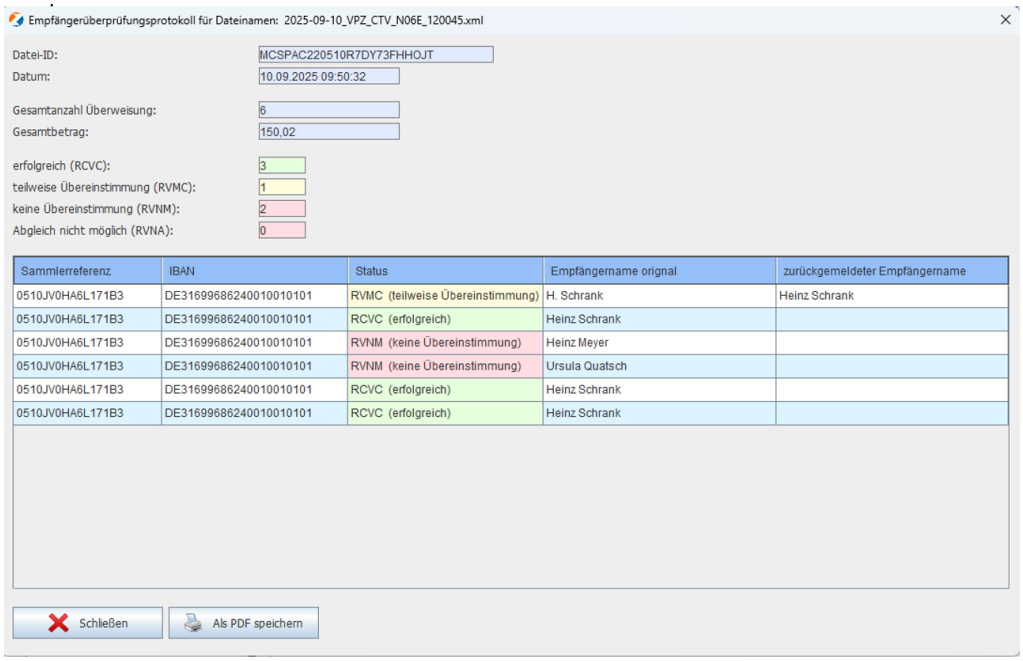


Abb. 5.34. VoP: Statusdatei

In der folgenden Abbildung ist die Anzeige derselben Statusdatei nach der Sortierung über die rot gekennzeichnete Tabellenspalte "Status" abgebildet:

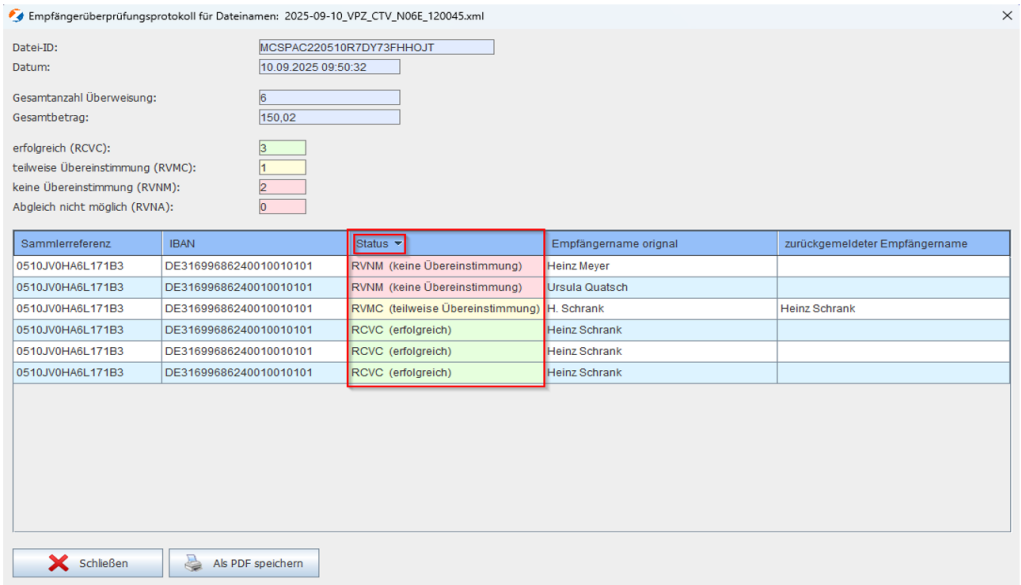


Abb. 5.35. VoP: Statusdatei sortiert nach dem Status

6. Anhang

6.1. Dateifilter

Zweck

Dateifilter spielen vor allem im Konsolenmodus eine wichtige Rolle. Sie sind notwendig, um bei Uploadaufträgen die Dateitypen herauszufiltern, die mit der eingestellten Auftragsart übertragen werden sollen. Dazu werden die 3-5-stelligen Dateiendungen gespeichert, die mit der jeweiligen Auftragsart übertragen werden sollen.

Standard-Einstellungen

Vorbelegt ist anfänglich das 3-stellige Kürzel der jeweiligen Auftragsart (z.B. "AZV").

Menüpunkt

Den Dateifilter-Editor erreichen Sie über den Reiter "Zugänge". Betätigen Sie zunächst die Schaltfläche "Vorbelegungen" und dann die Schaltfläche "Dateifilter f. Auftragsart".

Gültigkeit

Die Konfiguration der Dateifilter ist je Zugangs-ID für jede einzelne Upload-Auftragsart individuell einstellbar.

Beispiele

In der folgenden Tabelle sind einige Auftragsarten mit dafür typischen Dateiendungen aufgezählt:

Auftragsart	Typische Dateiendungen
AZV (Auslandszahlungsverkehr)	DTAZV
CCT	SEPA-XML

6.2. Rückgabewerte im Konsolenmodus

Allgemeines

Wenn MVSC mit Hilfe einer Batch-Datei verwendet wird, benötigt die aufrufende Anwendung Informationen über den Ausgang des Übertragungsvorgangs. Diese Information gibt MVSC in Form eines Zahlenwertes zurück, der wiederum eine bestimmte Meldung repräsentiert. Die verschiedenen Rückgabewerte und deren Bedeutung werden im Folgenden beschrieben.

Rückgabewerte und deren Bedeutung

Bei erfolgreicher Datenübertragung erhalten Sie als Rückgabewert die Zahl "1". Dieser Rückgabewert bedeutet, dass die Übertragung an den Bankrechner für alle gefundenen Dateien erfolgreich war.

Erhalten Sie als Rückgabewert die Zahl "0", so konnte mindestens eine gefundene Datei nicht erfolgreich übertragen werden. Meistens liegen dann Formatfehler in der entsprechenden Datei vor.

Rückgabewerte kleiner Null deuten dagegen auf einen Fehler in der vorgenommenen Konfiguration hin.

Die möglichen Rückgabewerte sind in der folgenden Tabelle dargestellt:

Rückgabewert	Bedeutung
25	Dieser Rückgabewert kann beim Programmstart im Konsolenmodus auftreten. In diesem Fall liegt ein Update für MVSC vor. Das Update kann nur im Desktop-Modus ausgeführt werden.

Rückgabewert	Bedeutung
1	Alle gefundenen Dateien wurden erfolgreich an den Bankrechner übertragen. Anschließend wurde auch das Kundenprotokoll (PTK/HAC) erfolgreich abgeholt.
0	Die Datenübertragung war nur teilweise erfolgreich. Mindestens eine der gefundenen Dateien konnte erfolgreich übertragen werden, andere Dateien allerdings nicht. Meistens sind Formatfehler in den Auftragsdateien der Grund für diesen Rückgabewert.
-1	Die EBICS-Zugangsdaten sind unvollständig oder fehlerhaft.
-2	Die Internet-Zugangsdaten sind fehlerhaft.
-3	Die eingetragene Auftragsart wird nicht unterstützt bzw. ist nicht für diese Zugangs-ID freigeschaltet.
-4	Es wurden laut Dateifilter im angegebenen Verzeichnis keine entsprechenden Dateien gefunden.
-5	Mindestens eine der gefundenen Dateien wird bereits von einem anderen Anwender übertragen (Netzwerkinstallation).
-6	Es wurden fehlerhafte Aufrufparameter übergeben.
-7	Es wurde eine Zugangs-ID übergeben, die als Signaturmedium eine Chipkarte verwendet. Im Konsolenmodus wird nur die Sicherheitsdatei unterstützt.
-8	Ein konfigurierter/ übergebener Verzeichnispfad ist entweder ungültig oder Sie besitzen keine Schreib- oder Leseberechtigung für diesen Verzeichnispfad.
-9	Die Anwendung wurde bereits gestartet. Die Datenübertragung wird verhindert, damit die vorliegenden Dateien nicht mehrfach übertragen werden.
-99	Sie verwenden eine Testversion, die nur einen bestimmten Bankrechner, aber nicht den übergebenen Bankrechner unterstützt.
-999	Ihre Programmversion ist abgelaufen und kann nicht mehr eingesetzt werden.

EBICS-Fehlermeldungen

Alle zurückgegebenen Zahlenwerte, die größer als 1 sind, weisen auf ein Problem hin, das vom EBICS-Server zurückgemeldet wurde. Diese Zahlen liegen meist im 5-stelligen Bereich und deuten auf Fehler hin, die im Zuge der EBICS-Übertragung aufgetreten sind. Tritt ein solcher Fehler auf, so wird die gesamte Übertragung abgebrochen, da beim Senden der nächsten Datei mit demselben Fehler zu rechnen wäre.

In der folgenden Tabelle sind einige dieser EBICS-Rückgabewerte und deren Bedeutung aufgeführt:

Rückgabewert/ EBICS-CODE	Spaltenüberschrift
90005/ EBICS_NO_DOWNLOAD_DATA_AVAILABLE	Auf dem EBICS-Bankrechner stehen keine Daten für diese Auftragsart zur Abholung bereit. Es handelt sich dabei nicht um einen Fehler, da es aus verschiedenen Gründen vorkommen kann, dass keine Daten verfügbar sind. Dies ist zum Beispiel der Fall, wenn die Daten bereits abgeholt wurden.
91002/ EBICS_INVALID_USER_OR_USER_STATE	Der sendende Teilnehmer ist dem Bankrechnersystem nicht bekannt oder wurde noch nicht am System freigeschaltet.
61001/ EBICS_AUTHENTICATION_FAILED	Für diese Fehlermeldung kann es verschiedene Ursachen geben: • Der sendende Teilnehmer ist nicht berechtigt, diese Auftragsart auszuführen.

Rückgabewert/ EBICS-CODE	Spaltenüberschrift
	• Der Benutzer hat seine privaten Schlüssel (INI) oder die öffentlichen Bankschlüssel (HPB) noch nicht mit dem Bankrechner synchronisiert. • Die Systeme arbeiten mit unterschiedlichen Zertifikaten.
91115/ EBICS_ORDERID_ALREADY_EXISTS	Jeder Auftrag wird mit einer eigenen Auftragsnummer (OrderID) übertragen. Diese darf sich innerhalb eines bestimmten Zeitraums nicht wiederholen. Wenn diese Meldung auftritt, wurden innerhalb weniger Tage zwei Aufträge mit der gleichen Auftragsnummer verschickt. Sie können dieses Problem beheben, indem Sie die Datei "Number.num" im "Konfig"-Vereichnis unterhalb des Installationsordners anpassen. Öffnen Sie dazu die Datei "Number.num" und erhöhen Sie den Wert des Elementes "BPZ" um mindestens 2. Beachten Sie dabei, dass der eingetragene Wert die Zahl 46655 nicht überschreiten darf. **Anmerkung** Ab der EBICS-Version 2.5 kann dieser Fehler nicht mehr auftreten, da die Auftragsnummern zentral am EBICS-Bankrechner vergeben werden.
90003/ EBICS_AUTHORISATION_ORDER_TYPE_FAILED	Der einreichende Teilnehmer ist für die ausgewählte Auftragsart nicht berechtigt. Möglicherweise wurde die Berechtigung für die Auftragsart am EBICS-Bankrechner entzogen. Um die Berechtigung für die Auftragsart zu bekommen, muss der Betreiber des EBICS-Bankrechners diese für den Teilnehmer freischalten. Anschließend ist es notwendig, über MVSC unter dem Reiter "Zugänge" die Schaltfläche "Auftragsarten abholen" zu betätigen, damit die am EBICS-Bankrechner vorgenommenen Änderungen auch in MVSC aktiv werden.

6.3. Auftragsarten

Auftragsarten in EBICS

Es wird zwischen Upload-Aufträgen (Übertragung zum EBICS-Server) und Download-Aufträgen (Abholung vom EBICS-Server) unterschieden.

Jede Auftragsart hat eine 3-stellige alphanumerische Kennung, über die sie eindeutig am EBICS-Bankrechnersystem identifiziert werden kann. Am EBICS-Bankrechner ist ebenfalls hinterlegt, welches Auftragsformat mit der jeweiligen Auftragsart übertragen werden soll und welche fachliche Verarbeitung mit den Daten durchgeführt wird.

Standard-Auftragsarten

Im EBICS-Standard sind für die gängigen Auftragsformate bereits diverse Auftragsarten vorgegeben worden.

In der folgenden Tabelle finden Sie Beispiele für originale EBICS-Auftragsarten:

Auftragsart	Übertragungsrichtung	Auftragsbeschreibung	Auftragsformat/ Verarbeitung
AZV	Upload	Senden AZV im Diskettenformat (Auslandszahlungsverkehr)	DTAZV
CCT	Upload	Senden Credit Transfer Initiation (SEPA-Überweisung)	pain.001

Auftragsart	Übertragungsrichtung	Auftragsbeschreibung	Auftragsformat/ Verarbeitung
CDD	Upload	Senden Direct Debit Initiation (SEPA-Basislastschrift)	pain.008
STA	Download	Abholen Swift-Tagesauszüge (Kontoumsätze)	MT940
VMK	Download	Abholen kurzfristige Vormerkposten	MT942
C52	Download	Abholen Bank To Customer-Account Report (Vormerkposten)	camt.052
C53	Download	Abholen Bank To Customer-Statement Report (Kontoumsätze)	camt.053

Es gibt noch weitere Auftragsarten, die durch den EBICS-Standard vorgegeben sind. Diese können Sie unter "http://www.ebics-zka.de/" einsehen.

6.4. Logging

6.4.1. Anwender-Logbuch

Aktionen des Anwenders

Alle Aktionen, die ein Anwender in der Benutzeroberfläche durchführt, werden im Anwender-Logbuch gespeichert. Damit die Aktionen chronologisch nachvollziehbar sind, wird für jeden Tag ein eigenes Anwender-Logbuch angelegt. Im Anwender-Logbuch sind keine technischen Informationen gespeichert, sondern hauptsächlich die während der Benutzung des Programms ausgegebenen Hinweis-Meldungen.

Menüpunkt

Das Anwenderlogbuch kann über den Reiter "Logbuch" eingesehen werden.

In der folgenden Abbildung ist der Reiter "Logbuch" dargestellt:

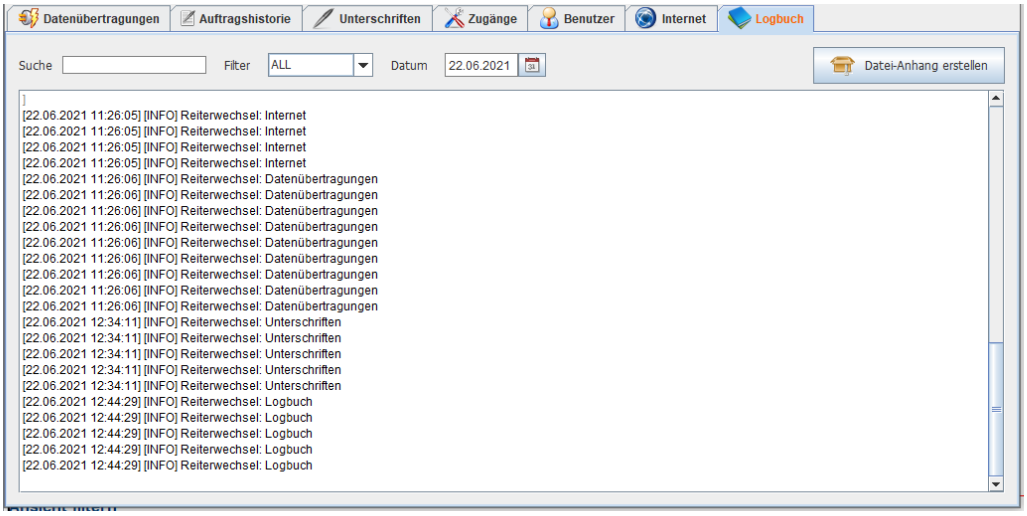


Abb. 6.1. Logbuch

Ansicht filtern

Wenn der Reiter "Logbuch" aufgerufen wird, werden zunächst die aktuellsten Logbuch-Einträge angezeigt. Mit Hilfe der Kalenderauswahl kann der Tag ausgewählt werden, für den das Anwenderlogbuch angezeigt werden soll. Über die Auswahlliste "Filter" kann die angezeigte Logbuch-Datei auf bestimmte Meldungstypen gefiltert werden. So kann schnell geprüft werden, ob z.B. an einem gewissen Tag Fehler (Filter "WARNING/ ERROR") aufgetreten sind.

Darüber hinaus kann das angezeigte Logbuch nach beliebigen Begriffen durchsucht werden.

Datei-Anhang erstellen

Falls es zu Problemen mit MVSC kommt, können die geschriebenen Log-Dateien über die Schaltfläche "Datei-Anhang erstellen" in ein ZIP-komprimiertes Dateiarchiv eingestellt werden. Diese Archivdatei kann dann an den Support der Atruvia AG weitergeleitet werden.

6.4.2. Technisches Logging

Log-Level

Wenn hartnäckige Probleme bei der Durchführung von Datenübertragungen auftreten, die auch nach mehreren Lösungsansätzen nicht behoben werden können, haben Sie die Möglichkeit, die Menge der geloggten Daten zu erhöhen. Es werden während des Verbindungsaufbaus detailliertere Informationen mitgeschrieben, die Aufschluss über den aufgetretenen Fehler geben können.

Diese Einstellung finden Sie im Menue "Hilfe", Unterpunkt "Logging". Sie haben vier verschiedene Möglichkeiten, den Log-Level einzustellen.

Diese möglichen Log-Level sind in der folgenden Abbildung dargestellt:

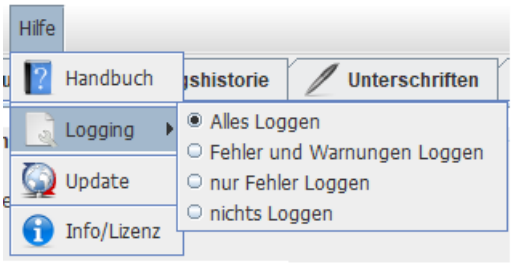


Abb. 6.2. Logging

Logdateien

Die Log-Dateien finden Sie im Unterverzeichnis "Traces". Die Dateien, die das technische Logging enthalten, beginnen mit dem Begriff "Trace". Die darin enthaltenen Informationen protokollieren ausschließlich den technischen Ablauf von EBICS-Datenübertragungen.

6.5. Hilfe

Handbuch

Unter dem Menuepunkt "Hilfe", "Handbuch" können Sie diese Anwenderdokumentation während der Nutzung von MVSC als PDF-Dokument aufrufen.