ITSG

dakota ag

dakota le

Benutzerhandbuch

Version 8.x0

Dokument: dakota BenutzerhandbuchV8.X0.docx, Druckdatum: 17.06.2026

Copyright

Die in diesem Handbuch enthaltenen Angaben und Daten können ohne vorherige Ankündigung geändert werden.

Die Informationen in diesem Handbuch dürfen ohne ausdrückliche Genehmigung der ITSG GmbH weder ganz noch teilweise für jegliche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, ob die Vervielfältigung oder Übertragung auf elektronischem, fotooptischem oder mechanischem Wege geschieht.

© ITSG GmbH 2026

Microsoft, Windows 11, MS Office sind eingetragene Marken der Microsoft Corporation.

Andere aufgeführte Produkte oder Firmennamen sind möglicherweise Marken oder eingetragene Warenzeichen ihrer jeweiligen Besitzer.

ITSG GmbH
Kaiserleistraße 10 – 16
63067 Offenbach

Inhaltsverzeichnis

1 Einleitung 5
1.1 dakota 5
1.2 Das Sicherheitsverfahren im Gesundheitswesen 6

2 Inbetriebnahme 7
2.1 Kurzbeschreibung 7
2.2 Installation 9
2.3 Inbetriebnahme mit dem dakota-Assistenten 14
2.3.1 Programmstart 14
2.3.2 Anmeldung am ITSG Registrierungsportal 15
2.3.3 Konfiguration der Versandart 17
2.3.3.1 Versandart Kommunikationsserver 18
2.3.3.2 Versandart dakota-E-Mail (SMTP) 18
2.3.3.3 Versandart dakota-E-Mail / Office 365 mit OAuth2 20
2.3.3.4 Versandart Verzeichnisausgabe 22
2.3.4 Konfiguration des Schlüssels (Zertifizierungsantrag) 23
2.3.4.1 Erfassen des verantwortlichen Ansprechpartners 24
2.3.4.2 Erfassen des Schlüssel-Passworts 24
2.3.4.3 Zusammenfassung der Angaben 25
2.3.4.4 Fertigstellen und Aussendung des Schlüssels an das ITSG-Trust Center 26
2.3.4.5 Einlesen der Zertifikatsantwort vom ITSG Trust Center 31

3 Verarbeitung 34
3.1 Kurzbeschreibung 34
3.2 Programmstart 35
3.3 Daten durch den Direktaufruf von dakota verarbeiten 36
3.3.1 Daten verarbeiten 36
3.3.2 Versenden über SOAP/MTOM (nur dakota.ag) 37
3.3.3 Versenden per E-Mail: dakota-E-Mail 37
3.3.4 Multitenant App Registration im Entra Admin Center mit OAuth2 37
3.3.5 Versenden über die Verzeichnis-Ausgabe 39
3.4 Verschlüsseln und Versenden integriert in die Fachanwendung 40

4 Protokollierung 41
4.1 Kurzbeschreibung 41
4.2 Langprotokoll 42
4.3 Kurzprotokoll 43
4.3.1 Detailansicht 43

5 dakota-Aktualisierung 45
5.1 Kurzbeschreibung 45
5.2 Neues Zertifikat 46

6 Konfiguration 47
6.1 Allgemeine Einstellungen 48
6.2 Einstellungen für die Verschlüsselung 49
6.3 Einstellungen für die Entschlüsselung 50
6.4 Einstellungen für das Stammdatenupdate 51
6.5 Einstellungen für den Kommunikationsserver (nur in dakota.ag) 52
6.6 Einstellungen für die Schlüsselsicherung 53
6.7 Zertifikatsverwaltung 54

6.8 Sicherung erstellen 56
6.9 Sicherung importieren 57
6.10 Eigene Schlüsseldaten 58
6.11 Statusabfrage 59
6.12 Journal 60

7 Häufig gestellte Fragen 61
7.1 Allgemeine Fragen zu dakota.ag 61
7.2 Allgemeine Fragen zu dakota.le 62
7.3 Technisch orientierte Fragen 64

1 Einleitung

1.1 dakota

dakota ist ein Programm zur Unterstützung der gesicherten Internet-Kommunikation zwischen Arbeitgebern bzw. „sonstigen Leistungserbringern" und den Sozialversicherungsträgern.

Die Auflagen der Datenschutzbeauftragten des Bundes und der Länder, Daten mit personenbezogenem Inhalt auf dem Transportweg zu sichern, werden durch die Anwendung eines Sicherheitskonzeptes der Sozialversicherungsträger erfüllt. Alle Nutzdaten werden vor dem Versand verschlüsselt.

Der Name dakota bezeichnet eine Produktfamilie der ITSG GmbH und steht als Akronym für '**Da**tenaustausch und **Ko**mmunikationen auf der Basis **T**echnischer **A**nlagen'.

Dieses Handbuch beinhaltet die Informationen für die Produkte dakota.ag und dakota.le.

1.2 Das Sicherheitsverfahren im Gesundheitswesen

Voraussetzung für den elektronischen Datenaustausch personenbezogener Daten ist, dass Vertraulichkeit, Integrität und Verbindlichkeit in gleicher Weise wie beim herkömmlichen papiergebundenen Abrechnungsverfahren (z. B. durch verschlossene Umschläge und persönliche Unterschriften) sichergestellt werden. Verschlüsselung und digitale Signatur auf der Grundlage kryptographischer Verfahren sind hierfür geeignete Maßnahmen.

Jeder Teilnehmer des Datenaustauschs verfügt über ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten (geheimen) Schlüssel. Der private Schlüssel ist nur dem Teilnehmer bekannt. Der öffentliche Schlüssel wird allgemein bekannt gegeben.

Die beiden Schlüssel des Teilnehmers stehen in einer besonderen Beziehung zueinander. Daten, die mit einem der beiden Schlüssel verschlüsselt werden, können nur mit dem anderen passenden Schlüssel wieder entschlüsselt werden. Dabei können sowohl der öffentliche als auch der private Schlüssel zum Ver- und Entschlüsseln verwendet werden.

Kommunikationspartner verschlüsseln mit dem öffentlichen Schlüssel des Empfängers Daten, so dass nur der Empfänger als Inhaber des privaten Schlüssels diese Daten entschlüsseln kann. Mit einem privaten Schlüssel können jedoch Daten nicht nur entschlüsselt, sondern auch verschlüsselt werden. Man spricht in diesem Fall von einer digitalen Signatur. Der Absender signiert die Daten mit seinem privaten Schlüssel, so dass jeder mit dem allgemein bekannten öffentlichen Schlüssel des Absenders die digitale Signatur prüfen kann. Aus diesem Grund kann die digitale Signatur die Funktion einer eigenhändigen Unterschrift übernehmen. Durch Prüfung der digitalen Signatur können Fälschungen der Daten zuverlässig erkannt werden.

Durch die Verwendung von Verschlüsselung und digitaler Signatur in den Datenaustauschverfahren wird sichergestellt, dass

- Daten vertraulich übermittelt werden,
- der Absender der Daten zuverlässig erkannt werden kann und
- die Unverfälschtheit der übertragenen Daten festgestellt werden kann.

Eine Voraussetzung für die Sicherheit des Verfahrens ist, dass jeder Teilnehmer seinen privaten Schlüssel vor unbefugtem Zugriff schützt. Andernfalls könnten Daten von einem Unbefugten entschlüsselt bzw. im Namen des Teilnehmers signiert werden. Für den Schutz seines privaten Schlüssels ist jeder Teilnehmer selbst verantwortlich.

Jeder Teilnehmer muss aber auch sicher sein können, für die Verschlüsselung der für den Kommunikationspartner bestimmten Daten, einen authentischen öffentlichen Schlüssel zu verwenden. Es muss verhindert werden, dass dem Absender, der zum Verschlüsseln den öffentlichen Schlüssel des Empfängers benötigt, ein anderer Schlüssel untergeschoben werden kann. Die Authentizität des öffentlichen Schlüssels muss deshalb von einer neutralen und vertrauenswürdigen Instanz, dem so genannten Trust Center, durch ein Zertifikat bestätigt werden.

2 Inbetriebnahme

2.1 Kurzbeschreibung

Bevor die Dateien verarbeitet werden können, muss Ihr dakota mit Ihren Daten konfiguriert werden. Hierzu gehören:

- **Die Installation der Software auf Ihrem Computer:**
  Die dakota-Software muss vor der Inbetriebnahme auf Ihrem Computer installiert werden. Die Installation der Software kann auf mehreren Wegen erfolgen. Die Installation wird mit einem Setup-Assistenten durchgeführt oder ist bereits im Setup des Abrechnungsprogramms Ihres Softwarehauses integriert.

- **Die Konfiguration:**
  dakota beinhaltet einen Assistenten, um die Versandart einzustellen und um Zertifikate beim ITSG-Trust Center zu beantragen.

- **Die Konfiguration Ihrer Versandart:**
  Es ist möglich, die Daten für die Sozialversicherungsträger über dakota-E-Mail oder Verzeichnisausgabe zu übertragen. dakota-E-Mail bietet Ihnen die Möglichkeit, die Daten direkt (per SMTP Protokoll oder OAuth2) zu versenden. Beim ersten Start von dakota haben Sie die Möglichkeit, die Versandart über den Assistenten einzurichten. Der Assistent führt Sie dann automatisch durch die Einrichtung und unterstützt Sie bei der Eingabe der notwendigen Daten.

  Im Arbeitgeberverfahren ist der Versand über dakota-E-Mail ein Ersatzverfahren und kann daher optional eingerichtet werden.
  Die Notwendigkeit zur Einrichtung des Ersatzverfahrens besteht allerdings nicht.

  Seit dem 01.01.2016 ist im Datenaustausch zwischen Arbeitgebern und Datenannahmestellen nur noch das Format eXTra zugelassen, welches nicht per E-Mail unterstützt wird.

- **Die Konfiguration Ihres Schlüssels:**
  Für den verschlüsselten Datenaustausch mit den gesetzlichen Krankenkassen ist es notwendig, einen Antrag auf Zertifizierung Ihres Schlüssels bei einem Trust Center zu stellen. Dieser Antrag besteht aus den folgenden Bestandteilen:

  - **die p10-Datei (Zertifizierungsanfragedatei)**,
    wird von dakota automatisch online an das ITSG Trust Center übertragen.
  - **Anmeldung am ITSG Registrierungsportal**
  - **Kopie des Betriebsnummernzuteilungsbescheides.**
    Den Betriebsnummernzuteilungsbescheid erhalten Sie von der Bundesagentur für Arbeit.

Wenn Sie einen Schlüssel als „sonstiger Leistungserbringer“ (Physiotherapie, Ergotherapie, etc.) beantragen möchten, benötigen Sie noch zusätzlich (bei der Erstbeantragung eines Zertifikats für ein Institutionskennzeichen-IK-) eine

- **Kopie des IK-Vergabebescheides.**

Den IK-Vergabebescheid erhalten Sie von der Arbeitsgemeinschaft Institutions-Kennzeichen in Sankt Augustin.

- **Das Einlesen der Antwort vom ITSG Trust Center:**
  Das ITSG Trust Center zertifiziert Ihren Schlüssel für die Teilnahme am Datenaustausch im deutschen Gesundheits- und Sozialwesen. Zusätzlich erhalten Sie vom ITSG Trust Center die Schlüssel der Datenannahmestellen, um die Daten entsprechend für den Empfänger zu verschlüsseln.

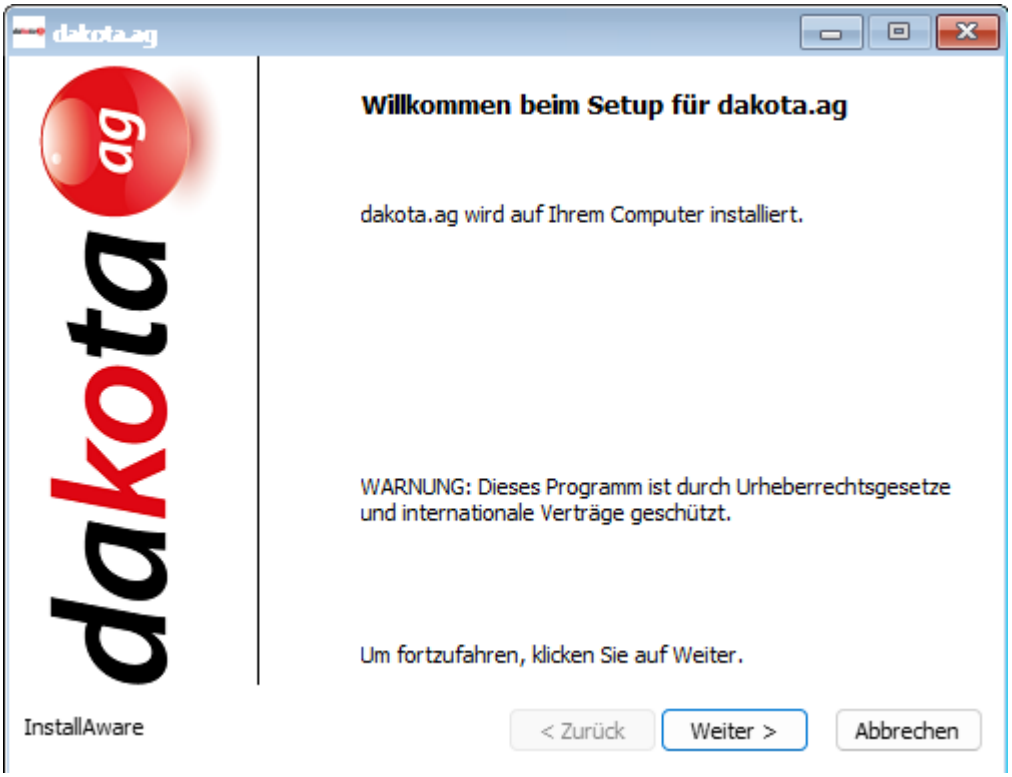
- **Das Versenden der Daten an die Sozialversicherungsträger und andere Empfänger:**
  Alle Dateien werden vor der Übermittlung sicher verschlüsselt und automatisch versendet. Im Arbeitgeberverfahren werden die Dateien per SOAP/MTOM an die Kommunikationsserver der Teilnehmer übermittelt.

  Im Leistungserbringerverfahren werden die Daten per E-Mail übertragen. Sie können über das Kurzprotokoll immer erkennen, welche Dateien von Ihnen bereits versendet wurden.

2.2 Installation

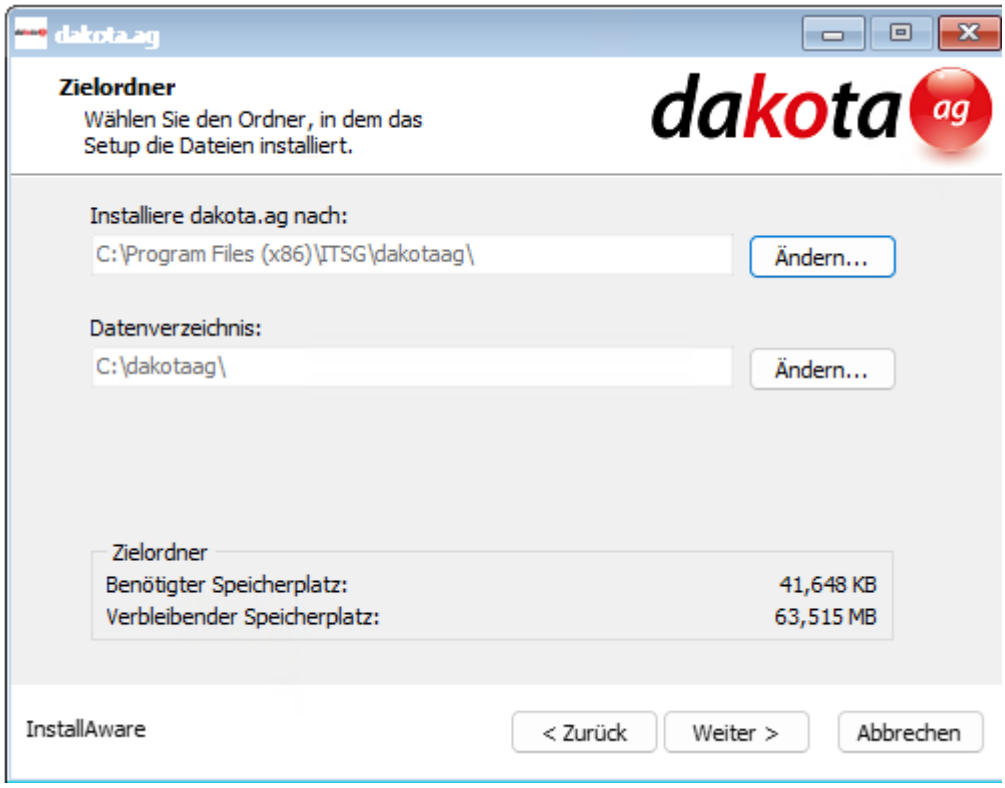
Die dakota-Software muss vor dem Einsatz auf Ihrem Computer installiert werden. Sie werden bei der Installation von dakota von dem Installations-Assistenten geleitet. Die Installation von dakota starten Sie bitte über das Programm **Setup.exe**.

Der Installations-Assistent begrüßt Sie und erläutert Ihnen, welche dakota-Variante und welche Version Sie installieren können.

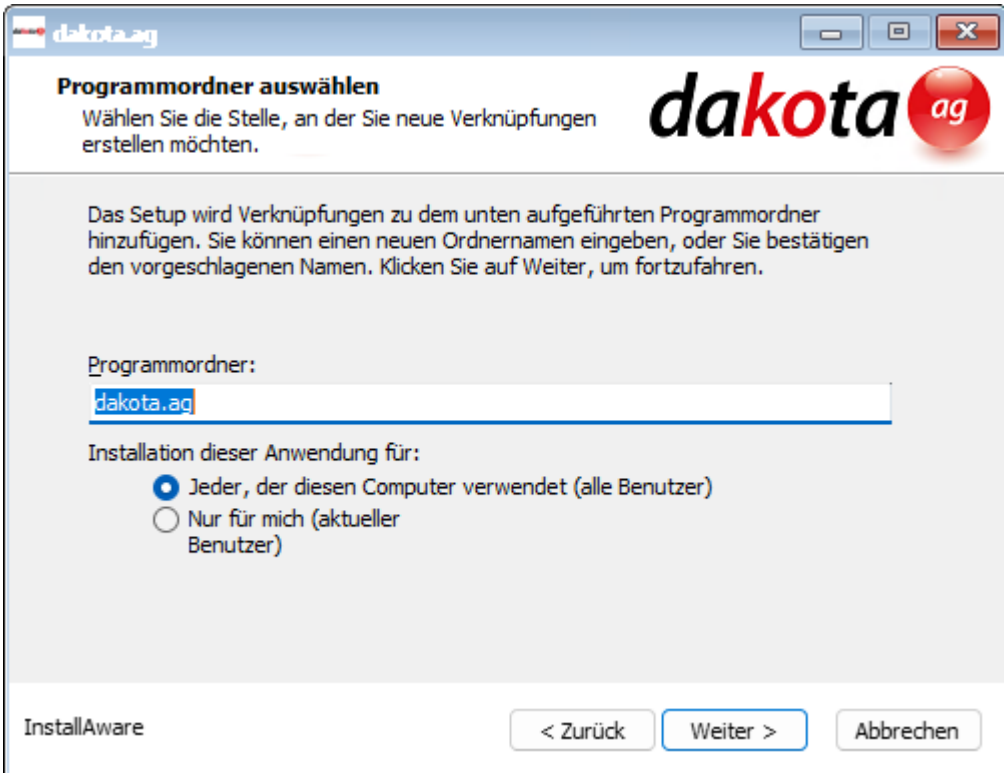


Wenn Sie die Installation beenden möchten, können Sie hierfür den Button Abbrechen nutzen.

Der Installations-Assistent wird nun den Programm-Pfad von dakota standardmäßig in das Verzeichnis (AG) **C:\Programme\ITSG\dakota.ag /** (LE) **C:\Programme\ITSG\dakota.le** und das Datenverzeichnis in (AG) C:\dakota.ag / (LE) C:\dakota.le installieren. Im Datenverzeichnis werden Ihre Benutzerdaten abgelegt, wie z. B. Ihre Verarbeitungsprotokolle. Wenn Sie die Pfade wechseln möchten, wählen Sie bitte Ändern... und ändern Sie die Pfadangabe auf das gewünschte Verzeichnis. Sobald Sie den gewünschten Programm-Pfad angegeben haben, wählen Sie bitte Weiter > um mit der Installation fortzufahren.



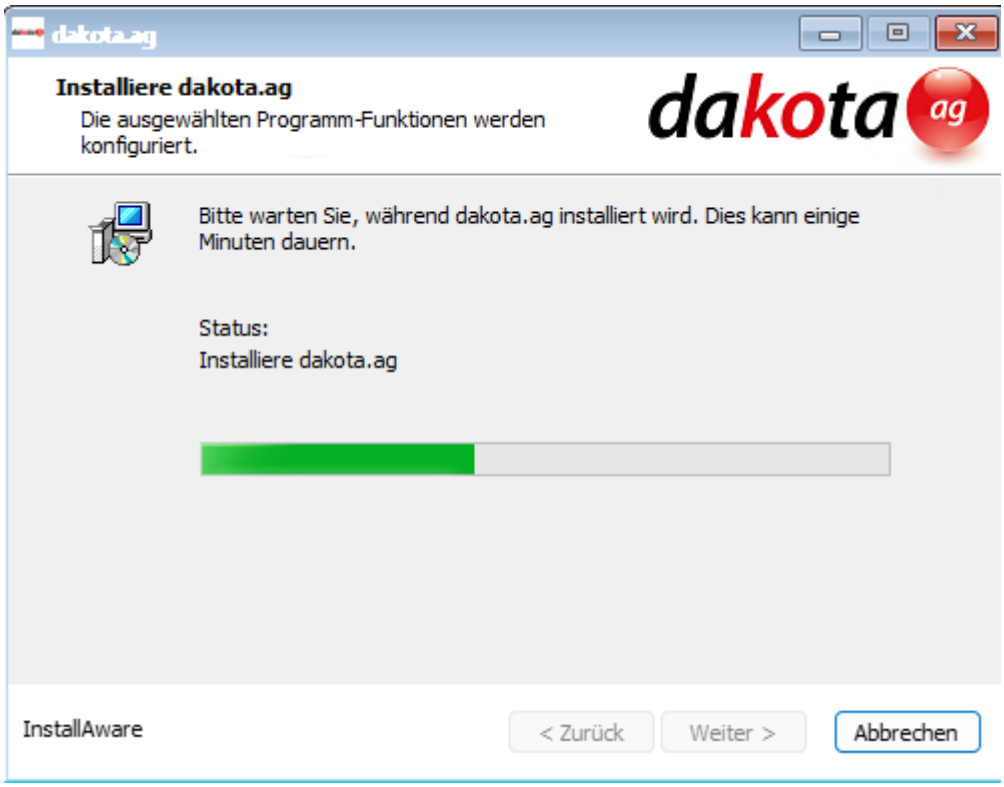
Auf der folgenden Maske können Sie eine gewünschte Bezeichnung für die Verknüpfung unter **Start/Programme** bzw. **Alle Programme** in Ihrem Windows Betriebssystem festlegen. Wählen Sie Weiter > um mit der Installation fortzufahren.



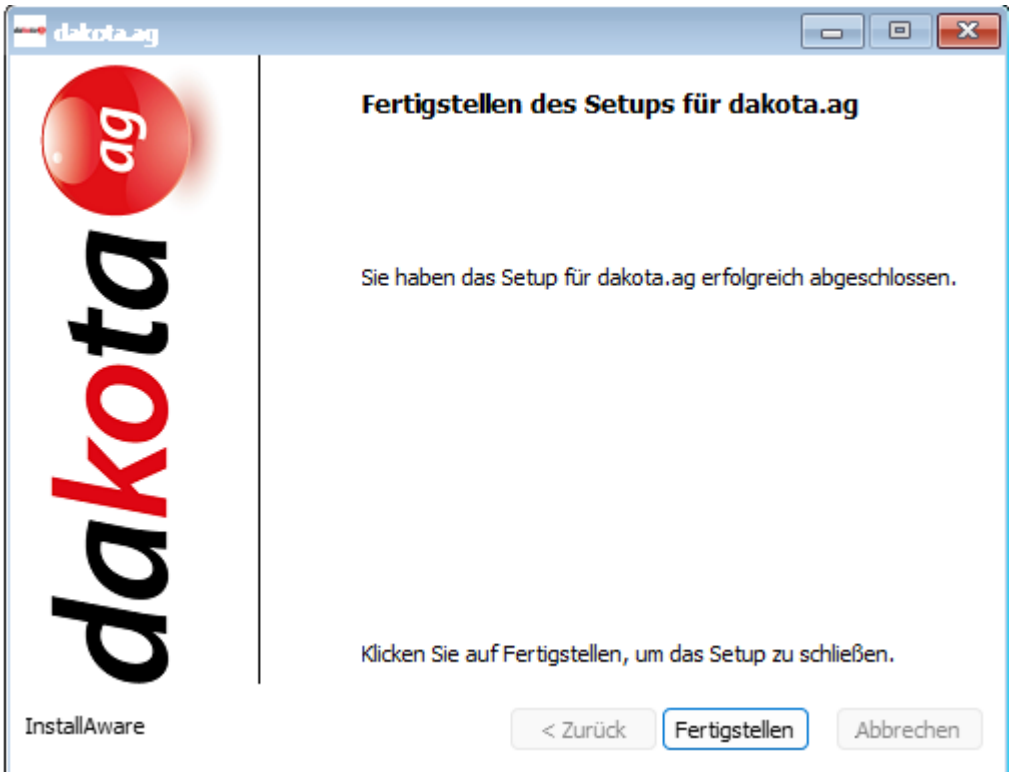
Auf der nächsten Maske werden Sie nochmals gefragt, ob die Installation durchgeführt werden soll. An dieser Stelle können Sie die Installation noch über Abbrechen beenden oder Weiter > starten.



Die Software wird nun auf Ihrem Computer installiert. Bitte haben Sie ein wenig Geduld. Die Installation ist abgeschlossen, wenn der Fortschrittsbalken vollständig durchgelaufen ist.



Abschließend informiert Sie der Installations-Assistent über die erfolgreiche Installation der dakota-Software. Wählen Sie Fertig stellen ,um die Installation abzuschließen. Fahren Sie nun mit der Inbetriebnahme mit dem dakota-Assistenten fort.



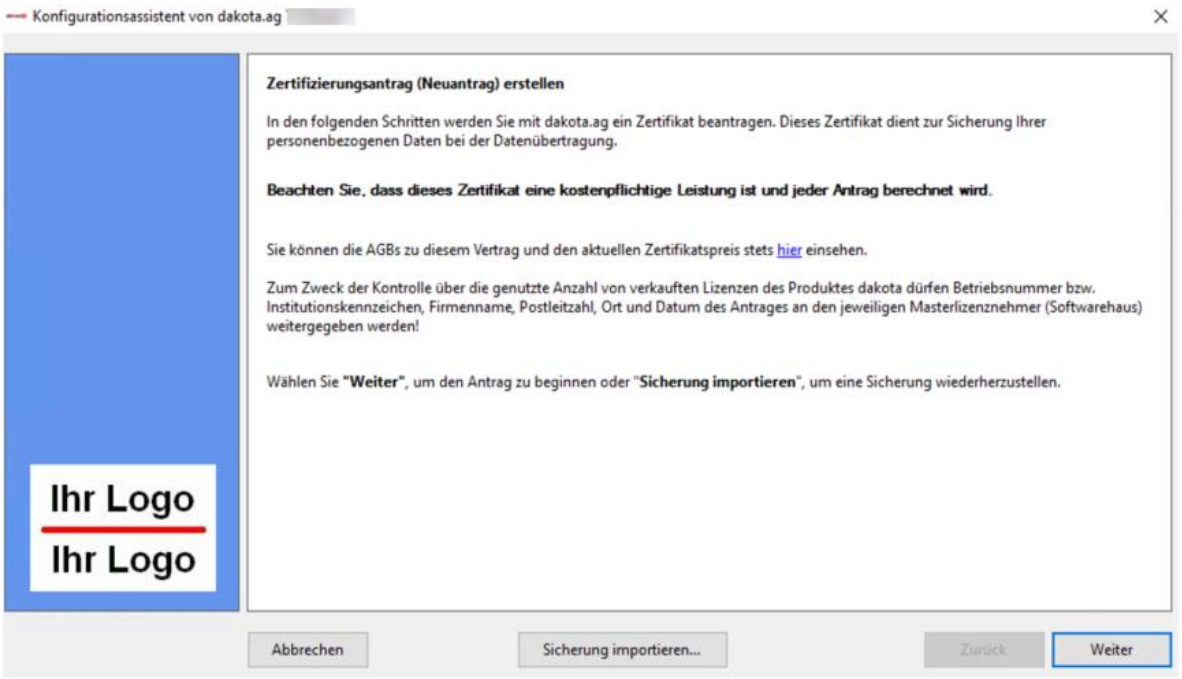
2.3 Inbetriebnahme mit dem dakota-Assistenten

2.3.1 Programmstart

Der dakota-Assistent wird in der Regel von Ihrem Softwarehaus in Ihre Fachanwendung eingebunden.
dakota können Sie wie folgt direkt aufrufen:
⇒ *'Start → Alle → dakota → dakota...'.*

Beim ersten Aufruf von dakota ist immer zuerst eine Registrierung erforderlich. Mit dieser Registrierung melden Sie Ihre dakota-Lizenz am Stammdatenupdateserver an. Die Registrierung dient dazu Ihre dakota-Installation zu lizensieren und alle Funktionen innerhalb der Anwendung zu aktivieren. Ohne die Registrierung ist es nicht möglich, dakota in Betrieb zu nehmen.

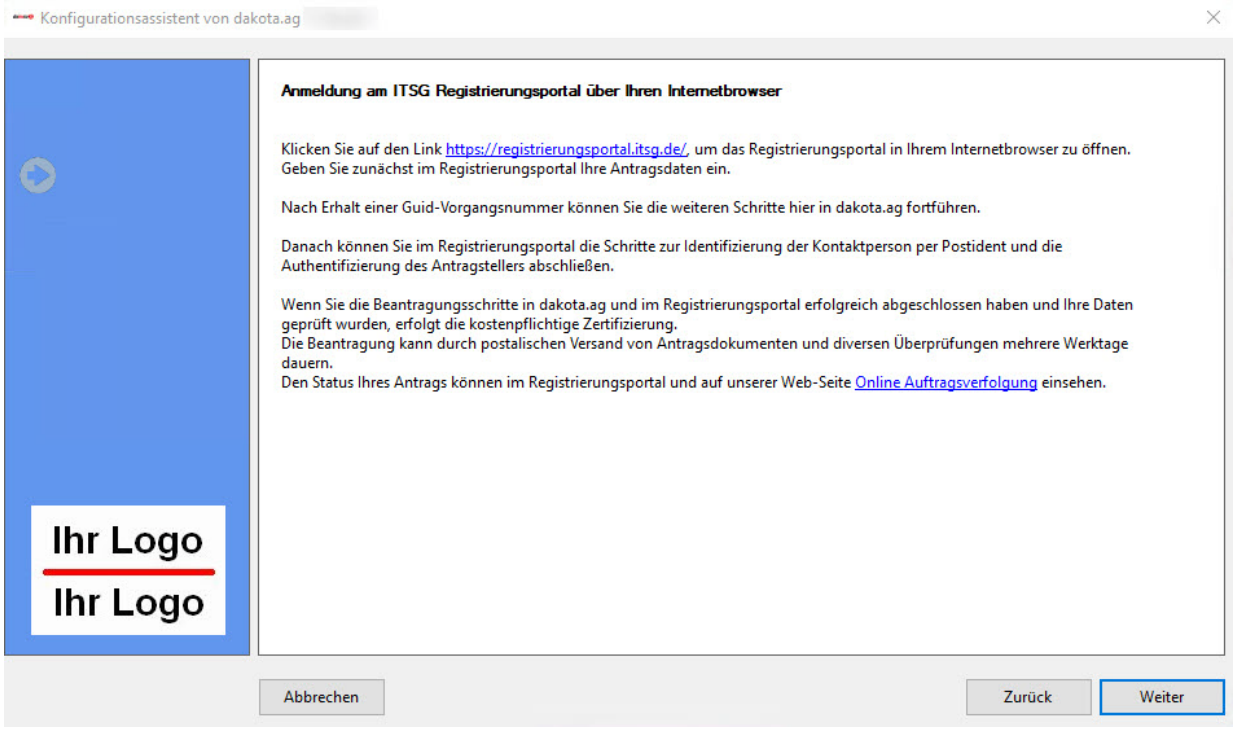
Nach der Registrierung und Freischaltung Ihrer installierten dakota-Lizenz führt Sie der Assistent schrittweise über den Button [Weiter] durch alle erforderlichen Punkte, die zur abschließenden Einrichtung von dakota notwendig sind. Die einzelnen Schritte sind in den folgenden Unterkapiteln beschrieben. Falls Sie einen Schritt im Assistenten wiederholen möchten, dann wählen Sie einfach die Funktion [Zurück] und korrigieren Sie Ihre Eingaben.



Sollten Sie bereits über eine Sicherung aus einer anderen Installation verfügen, so wählen Sie direkt [Sicherung importieren...] und importieren Sie diese.

2.3.2 *Anmeldung am ITSG Registrierungsportal*

Bitte klicken Sie auf den Link https://registrierungsportal.itsg.de; um den Browser zu öffnen.

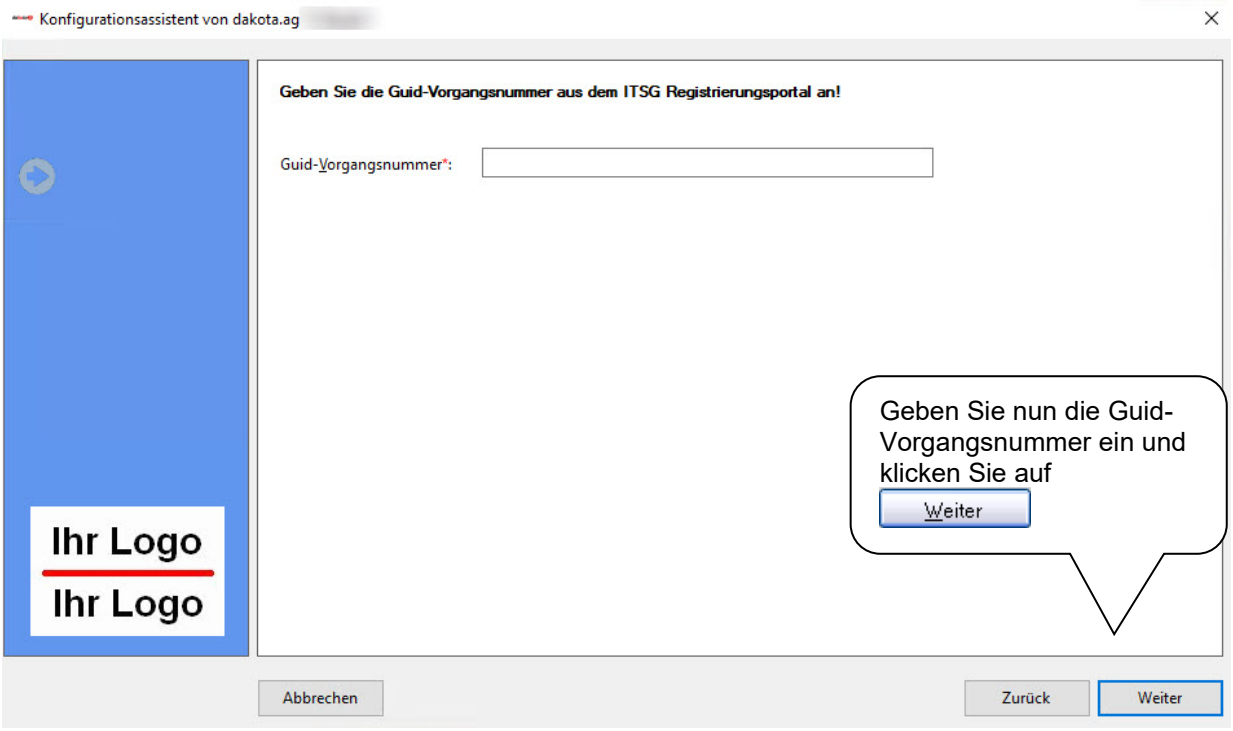


Handbuch zum Trust-Center-Registrierungsportal:

Trust-Center-Registrierungsportal-1.pdf

Videoanleitung zum Trust-Center-Registrierungsportal:

Videoanleitung Trust-Center-Registrierungsportal



Geben Sie die im ITSG-Registrierungsportal erzeugte Vorgangsnummer nach Durchführung der der oben aufgeführten Schritte ein. Anschließend klicken Sie auf Weiter.

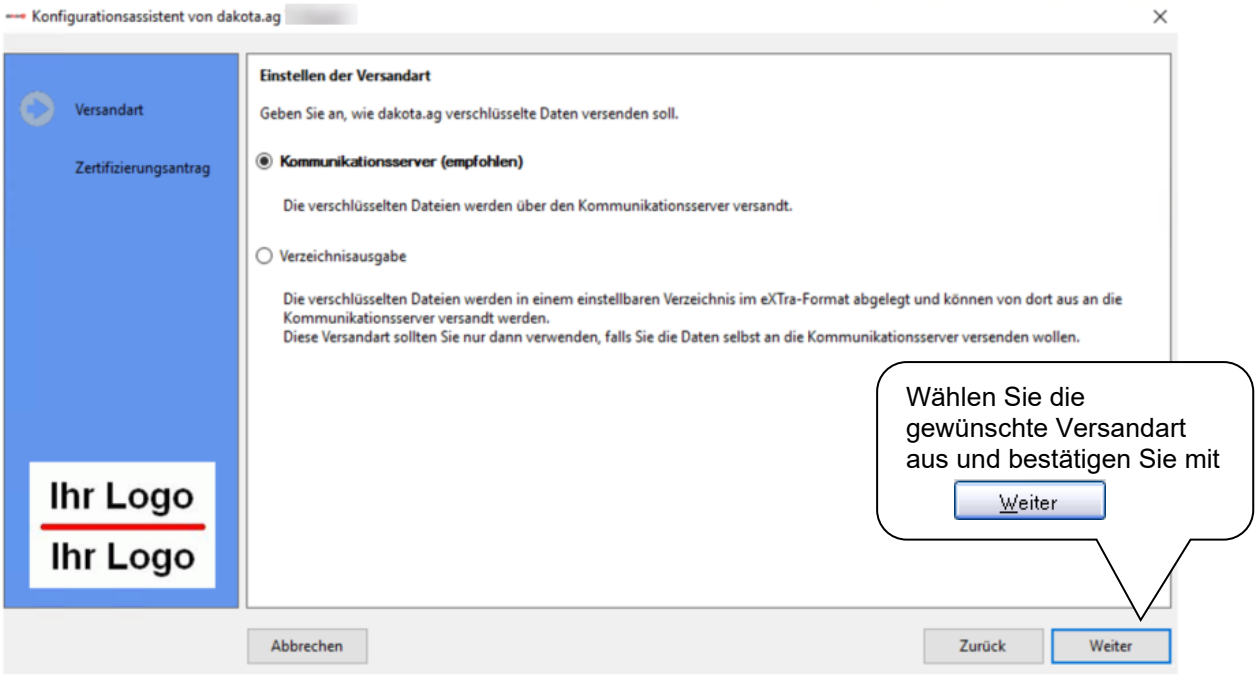
2.3.3 Konfiguration der Versandart

Damit Sie die verschlüsselten Dateien an die Datenannahmestellen der gesetzlichen Krankenversicherung übertragen können, müssen Sie in dakota einstellen, welche Versandart Sie verwenden möchten.

Die folgenden Versandarten stehen Ihnen zur Verfügung:

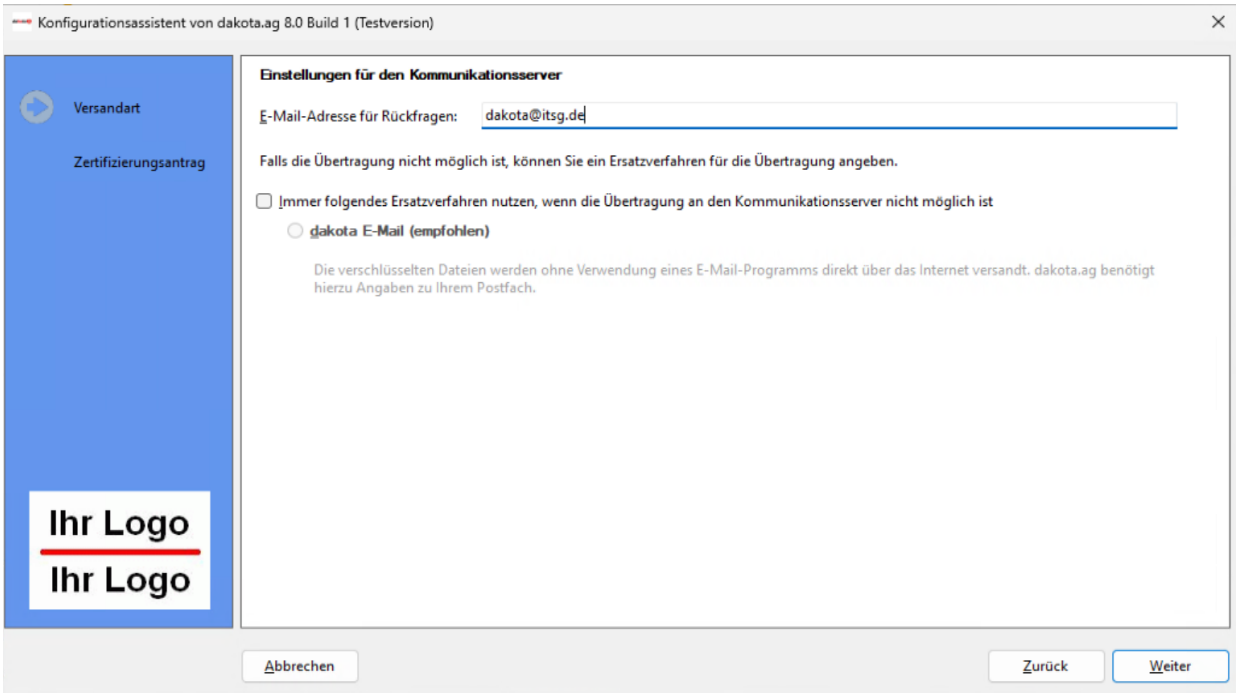
- **Kommunikationsserver (nur dakota.ag)**
  Diese Versandart überträgt Ihre Daten verschlüsselt über SOAP/MTOM direkt an die Kommunikationsserver der Datenannahmestellen.

- **Verzeichnisausgabe**
  Falls Ihnen die vorgenannte Versandart nicht zusagt, bieten wir Ihnen die Möglichkeit, die verschlüsselten Dateien in ein Ausgabeverzeichnis zu übergeben. Wenn Sie diese Versandart einstellen möchten, lesen Sie bitte im Kapitel 2.3.3.4 weiter.



2.3.3.1 Versandart Kommunikationsserver

Für die Versandart Kommunikationsserver müssen Sie eine E-Mail-Adresse für Rückfragen angeben.



Ebenfalls können Sie an dieser Stelle festlegen, ob als Übertragungsweg ein Ersatzverfahren erfasst werden soll. Folgende Versandarten stehen Ihnen als Ersatzverfahren zur Verfügung:

- **dakota-E-Mail (SMTP)**
  Diese Versandart arbeitet ähnlich wie Ihr E-Mail-Programm. Sie können über die Versandart die verschlüsselten Dateien direkt (über einen SMTP-Server) versenden. Wenn Sie diese Versandart einstellen möchten, lesen Sie bitte im Kapitel 2.3.3.2 weiter.

- **Multitenant App Registration im Entra Admin Center für OAuth2**
  Die Versandart übergibt die verschlüsselten Dateien komfortabel an Ihr Office 365. Wenn Sie diese Versandart einstellen möchten, lesen Sie bitte im Kapitel 2.3.3.3 weiter.

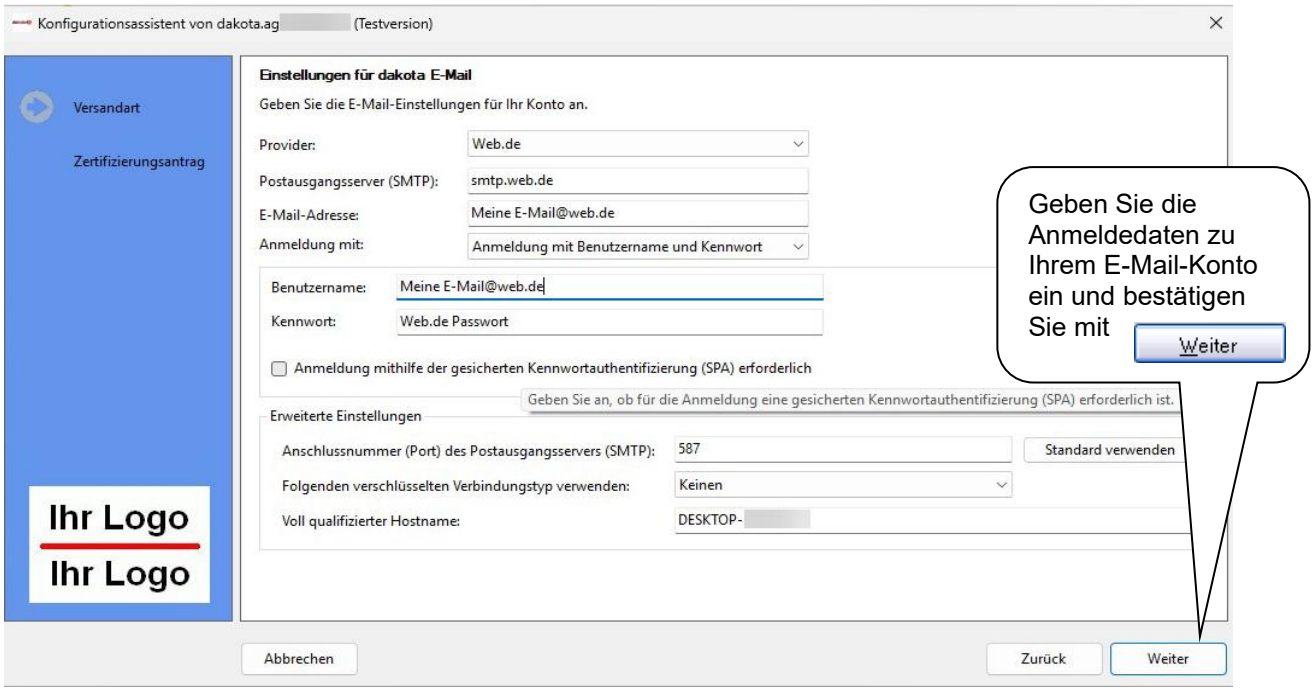
2.3.3.2 Versandart dakota-E-Mail (SMTP)

Für die Versandart dakota-E-Mail müssen Sie folgende Informationen in die dakota-Software eingeben:

- **SMTP-Server:** Geben Sie hier den Namen des SMTP-Servers Ihres E-Mail-Anbieters ein. Die Angaben des Namens erhalten Sie von Ihrem E-Mail-Anbieter oder fragen Sie ggf. bei Ihrem Softwarehaus nach.
  Hinweis: Sie finden in der Auswahlmöglichkeit **Provider** eine Liste der meistgenutzten E-Mail-Provider.

- **E-Mail-Adresse:** Bitte geben Sie in dieses Feld Ihre E-Mail-Adresse ein.

- **Server erfordert Authentifizierung:** Bei den meisten SMTP-Servern ist es notwendig, eine gesonderte Anmeldung mit Benutzername und Kennwort durchzuführen. Wenn der von Ihnen genutzte SMTP-Server diese Anmeldung verlangt, wählen Sie diese Option aus und geben Sie Ihren Benutzernamen und Ihr Kennwort für dieses E-Mail-Konto ein. Bei dieser Option fragen Sie ggf. bei Ihrem Systemadministrator oder dem Anbieter Ihres E-Mail-Kontos nach den Anmeldedaten.



- **Anschlussnummer (Port) des Postausgangsservers (SMTP):**
  Die Anschlussnummer für den Postausgangsserver ist standardgemäß der Port 25. Es ist möglich, dass manche Postausgangsserver eine andere Portadresse für das SMTP-Protokoll fordern.

- **Folgenden verschlüsselten Verbindungstyp verwenden:**
  Ein Postfach kann je nach Provider oder Einstellung eine unterschiedliche Verschlüsselung beim Verbindungsaufbau erfordern. Den Verbindungstyp können Sie bei Ihrem Provider oder Administrator erfragen und dann an dieser Stelle anschließend auswählen.

Falls Ihnen durch das Ausprobieren der Parameter die Ursprungswerte nicht mehr bekannt sind, können Sie mit der Funktion Standard verwenden die Angaben wieder auf den Auslieferungszustand zurücksetzen.

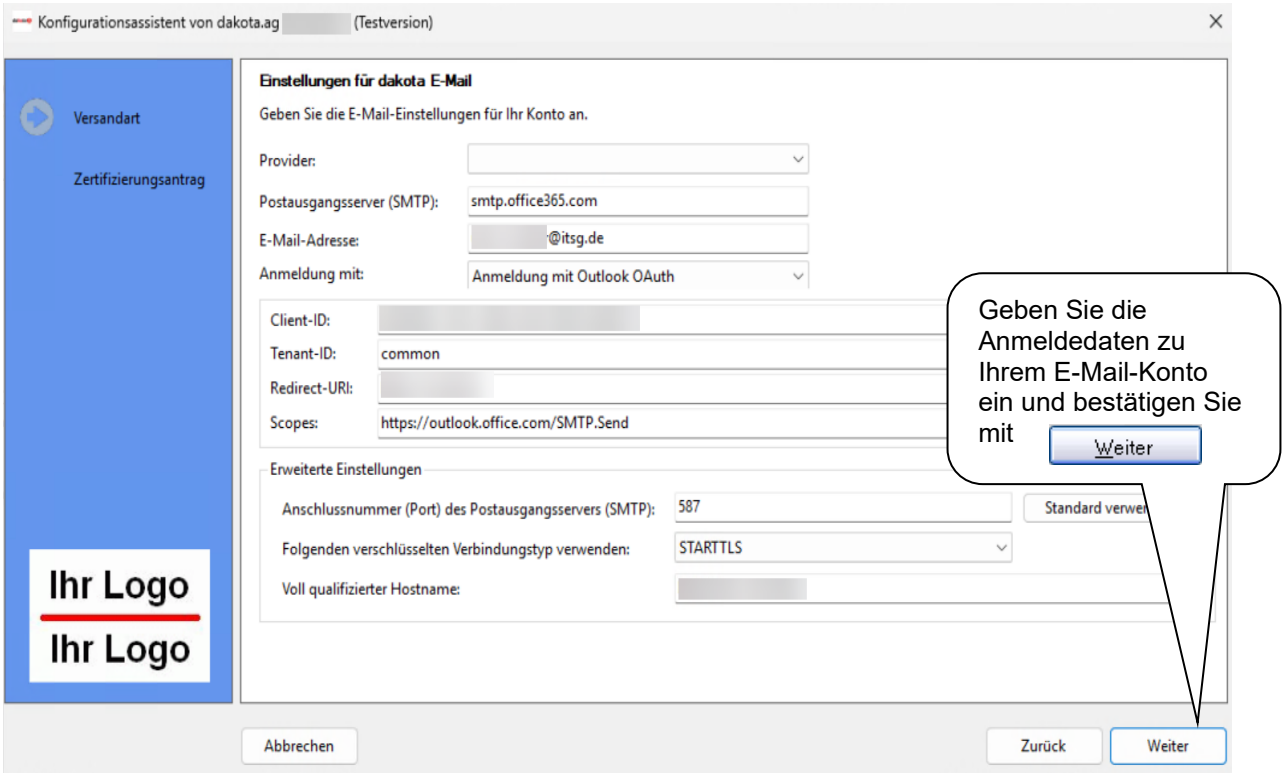
Wenn Sie nun alle Angaben zu Ihrem E-Mail-Konto eingerichtet haben, versucht dakota Ihre Versandart zu testen. Hierbei versendet dakota eine Test-E-Mail an die E-Mail-Adresse info-pas@itsg.de.

Hinweis: Bei dieser Test-E-Mail werden keine persönlichen Daten oder Registrierungsinformationen an das Internet gesendet. Der Test dient lediglich dazu, um technisch sicherzustellen, dass die Angaben zu Ihrem E-Mail-Konto korrekt eingegeben wurden.

Wenn die Versandart erfolgreich eingerichtet wurde, wird in den folgenden Schritten Ihr Schlüssel erzeugt und ein Antrag beim ITSG-Trust Center gestellt. Bitte lesen Sie nun im Kapitel 2.3.4 weiter, um die Konfiguration Ihres Schlüssels durchzuführen.

2.3.3.3 Versandart dakota-E-Mail / Office 365 mit OAuth2

Wenn Sie die Versandart dakota-E-Mail nutzen möchten, müssen Sie die folgenden Informationen in die dakota-Software eingeben:



Im Anschluss versucht dakota Ihre Versandart zu testen. Hierbei versendet dakota eine Test-E-Mail an die E-Mail-Adresse info-pas@itsg.de.

Viele E-Mail-Programme und Betriebssysteme verfügen über Sicherheitsmechanismen, um Ihren Computer gegen die Verbreitung von Viren zu schützen. Erlauben Sie bitte den Zugriff für

die dakota-Software. Wenn Sie die Nutzung Ihres E-Mail-Programms gestattet haben, finden Sie ggf. die Test-E-Mail in Ihrem Postausgang.

Hinweis: Bei dieser Test-E-Mail werden keine persönlichen Daten oder Registrierungsinformationen an das Internet gesendet. Der Test dient lediglich dazu, um technisch sicherzustellen, dass der Versand über Ihr E-Mail-Konto funktioniert.

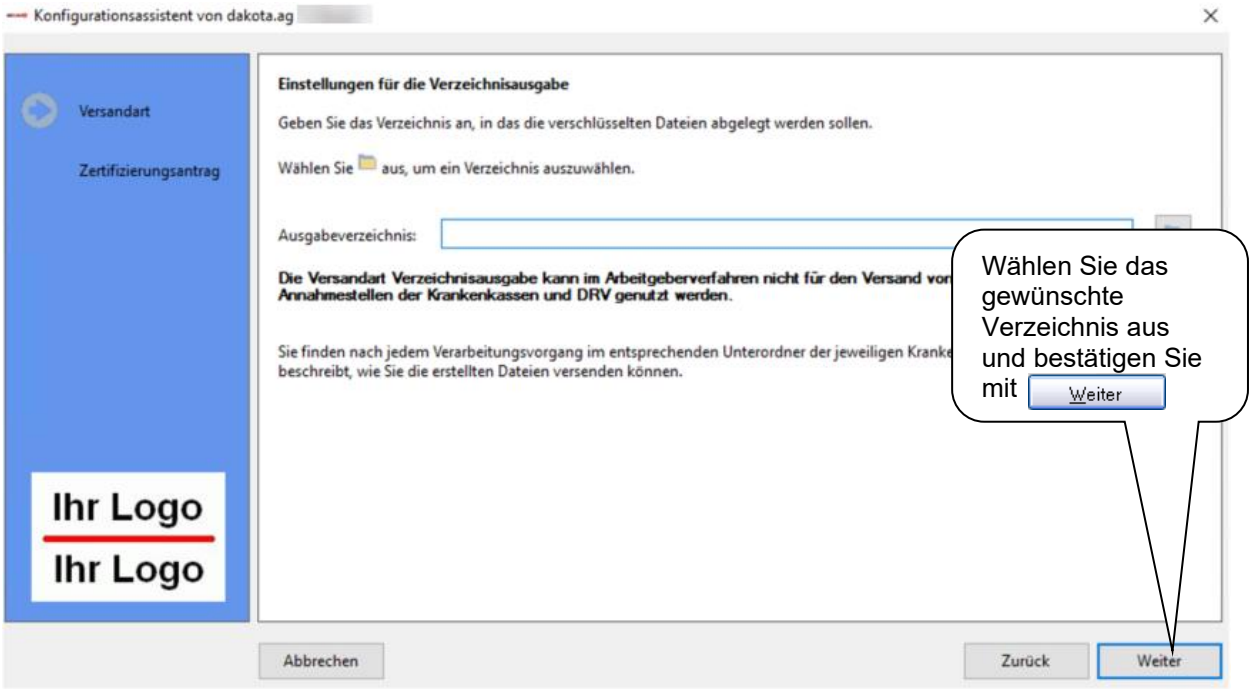
Wenn die Versandart erfolgreich eingerichtet wurde, wird in den folgenden Schritten Ihr Schlüssel erzeugt und ein Antrag beim ITSG-Trust Center gestellt. Bitte lesen Sie nun im Kapitel 2.3.4 weiter, um die Konfiguration Ihres Schlüssels durchzuführen.

2.3.3.4 Versandart Verzeichnisausgabe

Für die Versandart Verzeichnisausgabe müssen Sie die folgenden Informationen in die dakota-Software eingeben:

- **Verzeichnis:**
  Wählen Sie ein Verzeichnis als Ausgabeverzeichnis aus, dass dakota zukünftig die verschlüsselten Nachrichten für den manuellen Versand bereitstellen soll.

Hinweis Bitte stellen Sie sicher, dass Sie ausreichend Schreibrechte im angegebenen Verzeichnis besitzen. Fragen Sie ggf. Ihren Systemadministrator nach fehlenden Rechten.



Im Anschluss überprüft dakota ob die Zugriffsrechte auf das ausgewählte Ausgabeverzeichnis ausreichend sind.

Wenn die Versandart erfolgreich eingerichtet wurde, wird in den folgenden Schritten Ihr Schlüssel erzeugt und ein Antrag beim ITSG-Trust Center gestellt. Bitte lesen Sie nun im Kapitel 2.3.4 weiter, um die Konfiguration Ihres Schlüssels durchzuführen.

2.3.4 Konfiguration des Schlüssels (Zertifizierungsantrag)

Sie benötigen einen zertifizierten Schlüssel von einem Trust Center, um am elektronischen Datenaustausch mit der gesetzlichen Krankenversicherung teilnehmen zu können. Die dakota-Software bietet Ihnen die Möglichkeit, mit dem Assistenten die Einrichtung Ihres Schlüssels vorzunehmen. Für die Zertifizierung sind einige Angaben notwendig.

- **Wenn Sie Beitragsnachweise oder DEÜV-Meldungen an die GKV versenden möchten,**

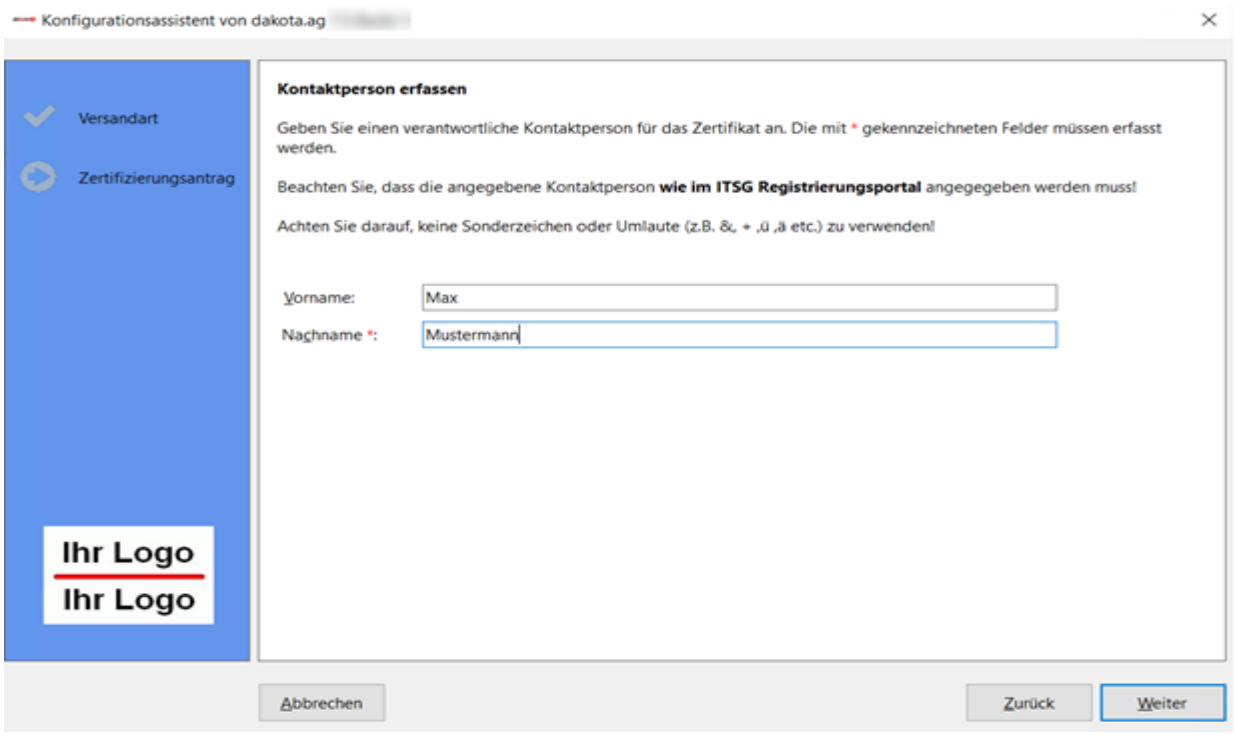
  geben Sie bitte auf der Maske Ihre **Betriebsnummer (BN)** ein. Eine Betriebsnummer erhalten Sie als Arbeitgeber von der lokalen Bundesagentur für Arbeit.

- **Wenn Sie Leistungsabrechnungen versenden möchten,**

  geben Sie bitte auf der Maske Ihr **Institutionskennzeichen (IK)** ein. Institutionskennzeichen werden von der SVI Arbeitsgemeinschaft Institutionskennzeichen, Alte Heerstraße 111, 53757 Sankt Augustin, vergeben.

Ebenfalls werden Sie auf der Maske nach Ihren Adressangaben gefragt. Alle Datenfelder, die mit einem * gekennzeichnet sind, müssen Sie ausfüllen.

Bitte beachten Sie, dass Sie keine Sonderzeichen (z. B.: +, /, *, etc.) bei der Eingabe Ihrer Adressdaten verwenden dürfen. Umlaute wie ä, ö und ü werden automatisch in ae, oe und ue umgewandelt.

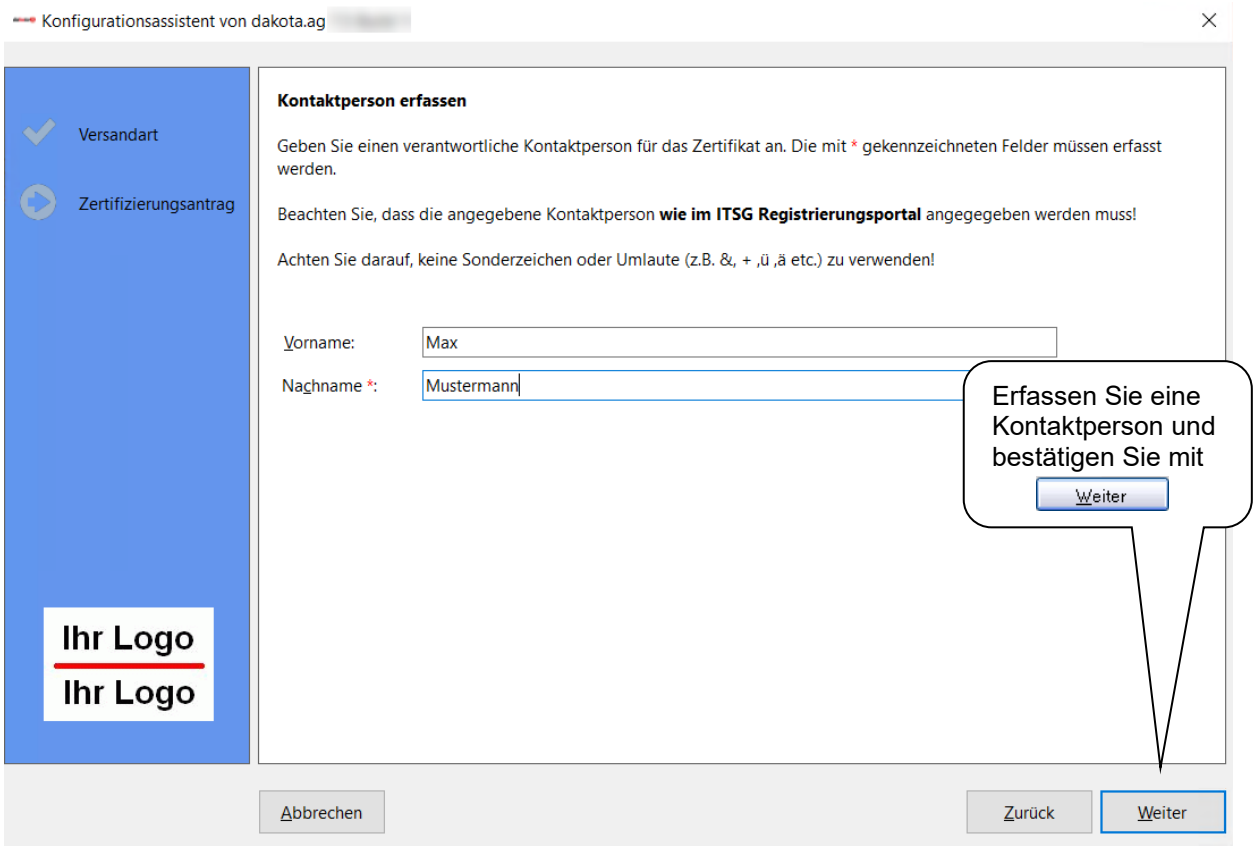


Hinweis: sollte das Feld „Nummer“ durch die BN-Nummer 12345678 oder durch die IK-Nummer 123456789 vorbelegt sein, so haben Sie eine Testversion von dakota im Einsatz.

2.3.4.1 Erfassen des verantwortlichen Ansprechpartners

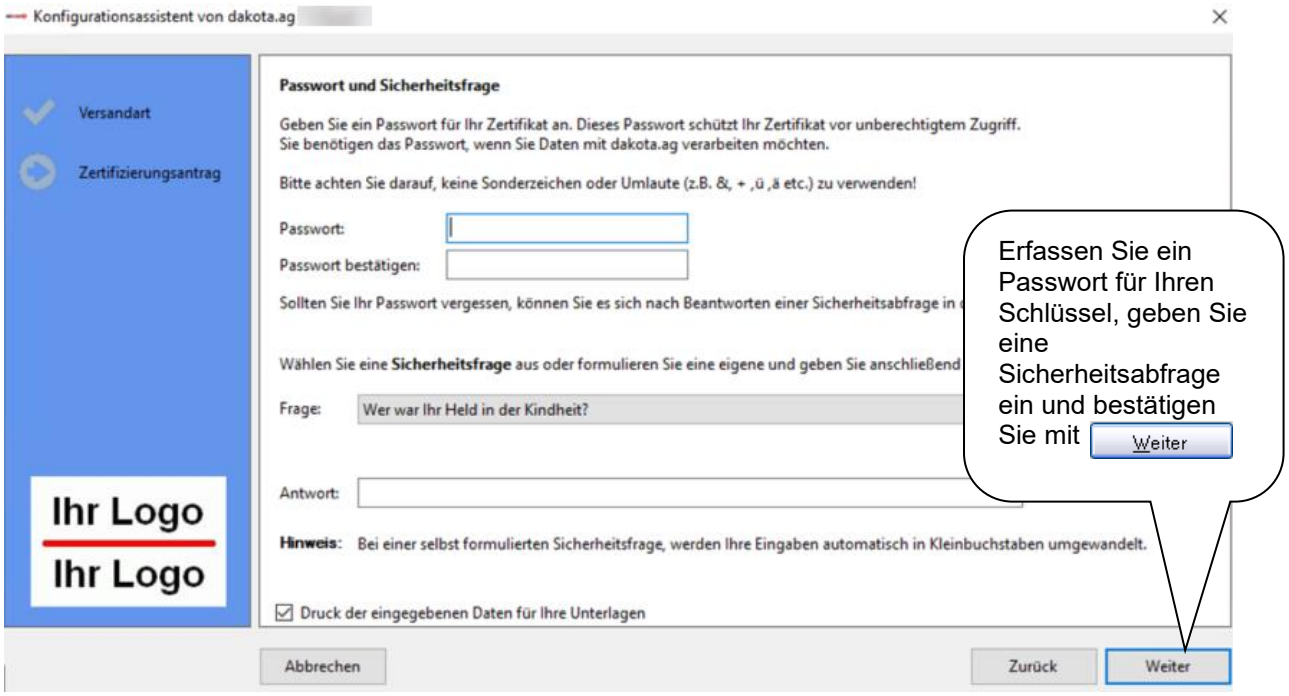
Im folgenden Schritt müssen Sie einen verantwortlichen Ansprechpartner für den Schlüssel benennen. Dieser verantwortliche Ansprechpartner muss immer eine natürliche Person sein.

Bitte verwenden Sie keine Sonderzeichen (z. B.: +, /, *, etc.) bei der Eingabe Ihrer Adressdaten. Umlaute wie ä, ö und ü werden automatisch in ae, oe und ue umgewandelt.



2.3.4.2 Erfassen des Schlüssel-Passworts

Damit Ihr Schlüssel vor unberechtigtem Zugriff geschützt wird, müssen Sie ein Passwort vergeben. **Bitte merken Sie sich das Passwort!** Bei jedem späteren Verschlüsseln und Versenden von Dateien werden Sie aufgefordert dieses Passwort einzugeben.



Hinweis: Das Passwort muss zwischen 6 und 9 Zeichen lang sein und darf keine Sonderzeichen (z. B. ü, ö, ä, +, etc.) enthalten. Beachten Sie bitte, dass sich nach der Eingabe das Passwort nicht mehr ändern lässt. Sollten Sie Ihr Passwort vergessen haben, können Sie es sich nach Beantwortung einer Sicherheitsabfrage in dakota anzeigen lassen. Die Sicherheitsabfrage wird Ihnen angezeigt, wenn Sie das Passwort dreimal falsch eingegeben haben.

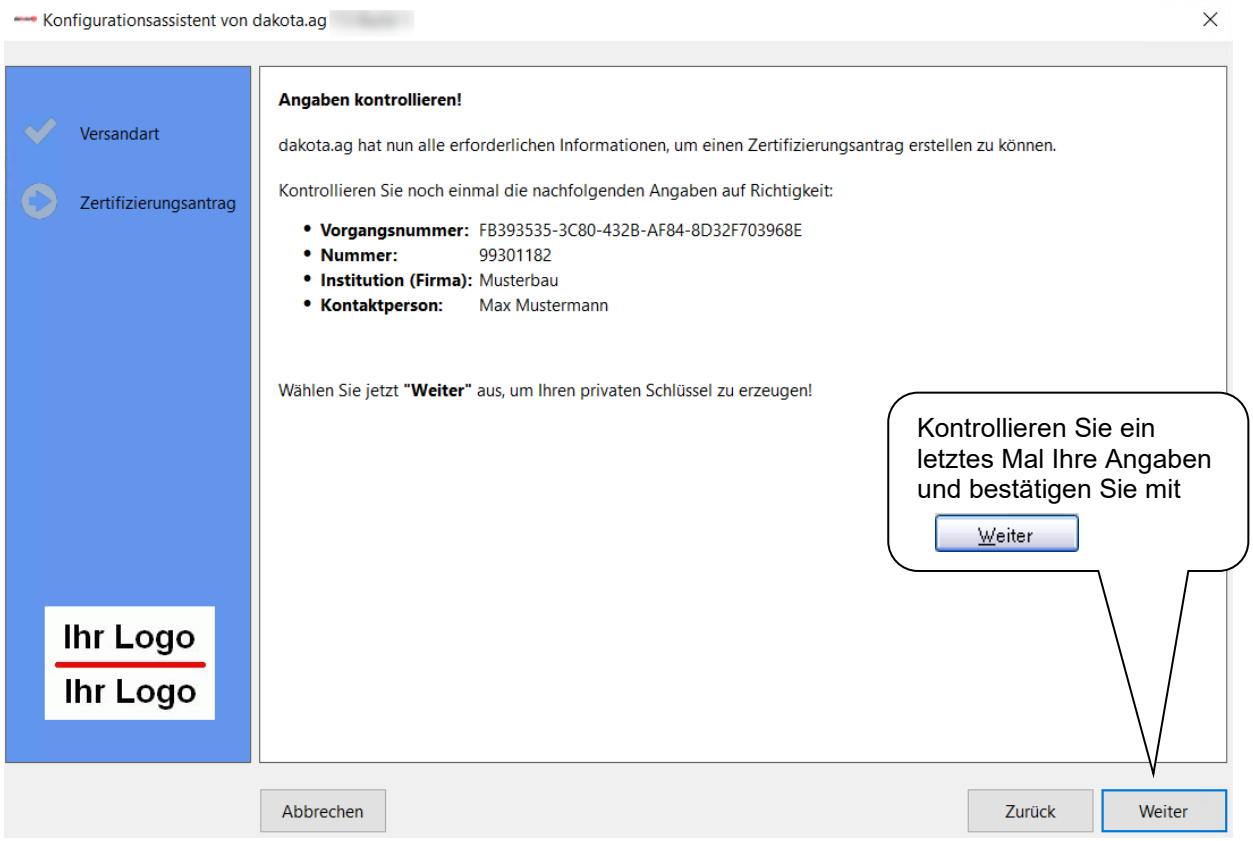
Die dakota-Software wird Ihre eingegebenen Informationen ausdrucken. Bitte beachten Sie, dass Sie diesen Ausdruck **nicht** an das ITSG-Trust Center senden. Auf diesem Ausdruck befinden sich Ihre persönlichen Angaben inklusive des Passwortes. Stellen Sie sicher, dass niemand außer Ihnen diesen Papierausdruck einsehen oder an sich nehmen kann.

Wenn Sie keinen Ausdruck Ihrer Angaben wünschen, dann entfernen Sie bitte den Haken bei ☑ Druck der eingegebenen Daten für ihre Unterlagen ta wird Ihre persönlichen Angaben nicht ausdrucken.

2.3.4.3 Zusammenfassung der Angaben

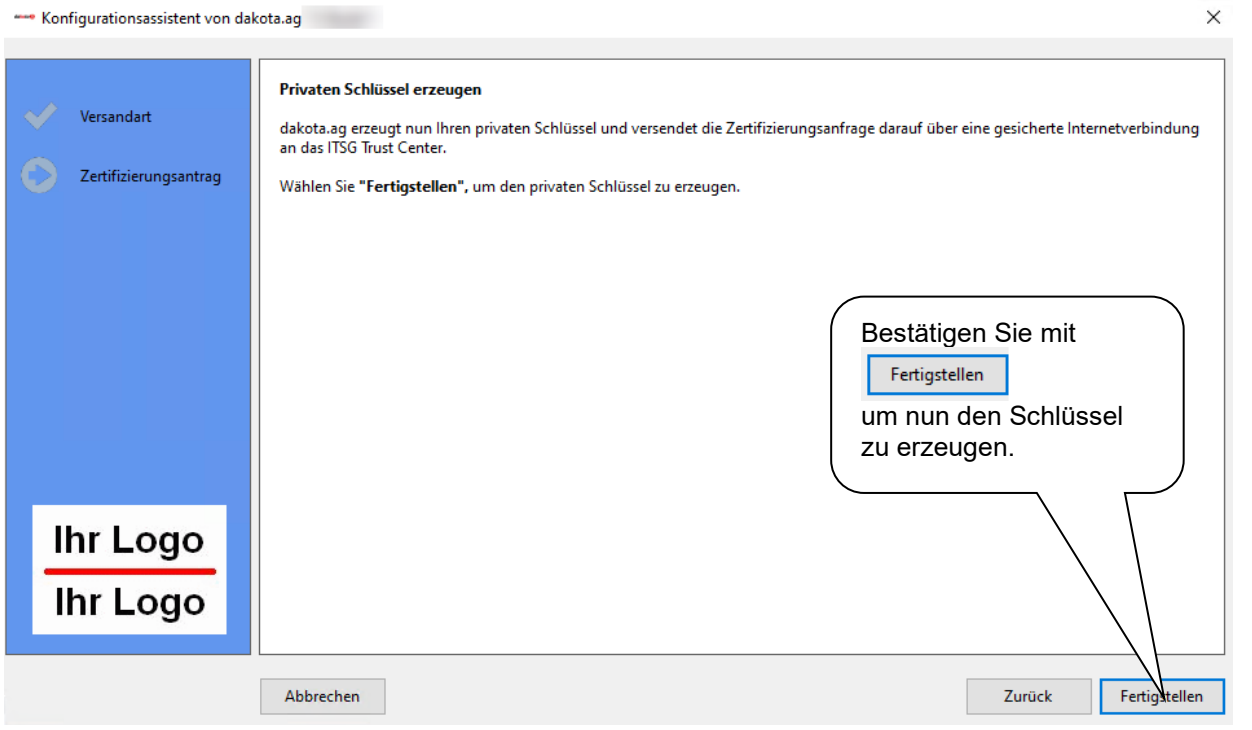
Zum Abschluss der Konfiguration Ihres Schlüssels zeigt Ihnen dakota alle Angaben noch einmal am Bildschirm an. Wenn Sie noch Fehleingaben entdecken und ggf. Korrekturen vornehmen möchten, können Sie mit Zurück wieder an jede Stelle im Assistenten zurückspringen.

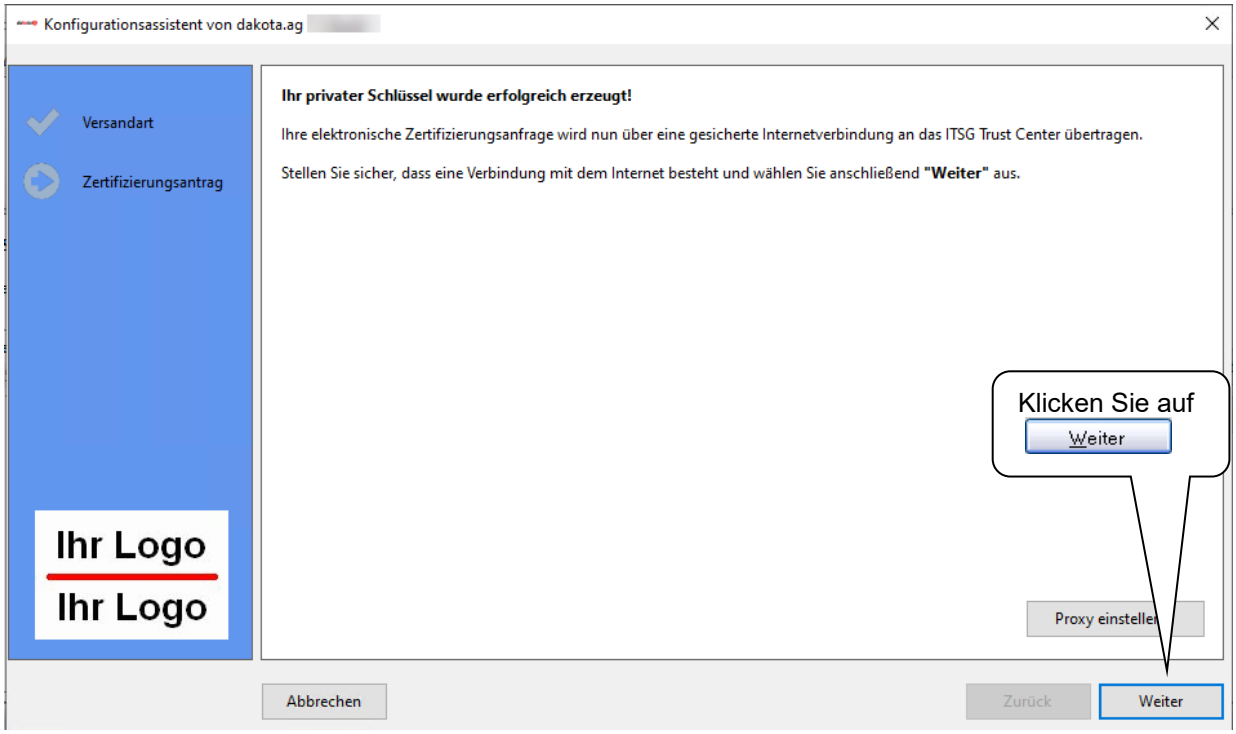
Bitte beachten Sie, dass ein Antrag auf Zertifizierung eine kostenpflichtige Leistung ist und jeder Antrag separat berechnet wird!



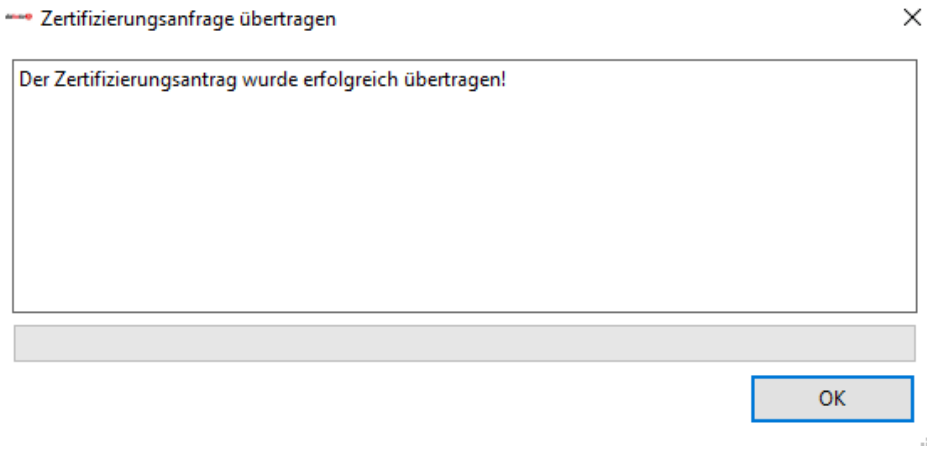
2.3.4.4 *Fertigstellen und Aussendung des Schlüssels an das ITSG-Trust Center*

Wenn alle Ihre Angaben korrekt sind, erstellt dakota nun Ihren Schlüssel.

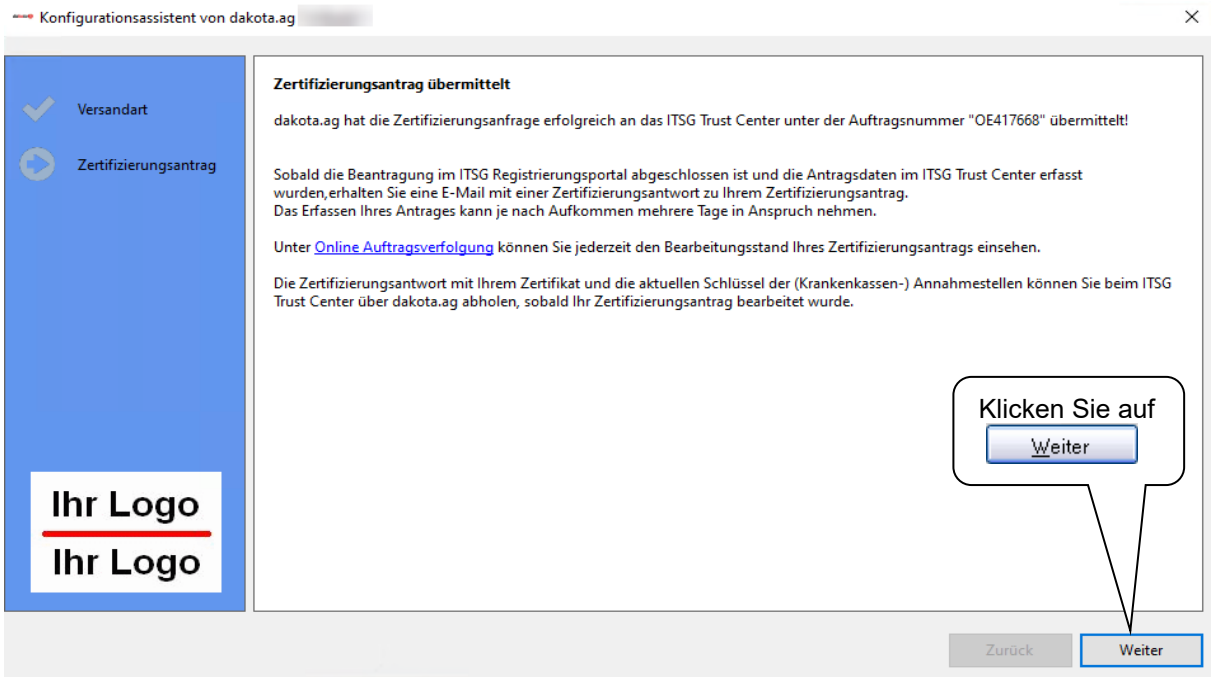




Nachdem der Schlüssel erfolgreich erzeugt wurde, wird dieser nun an das ITSG-Trust Center via Internet übertragen.

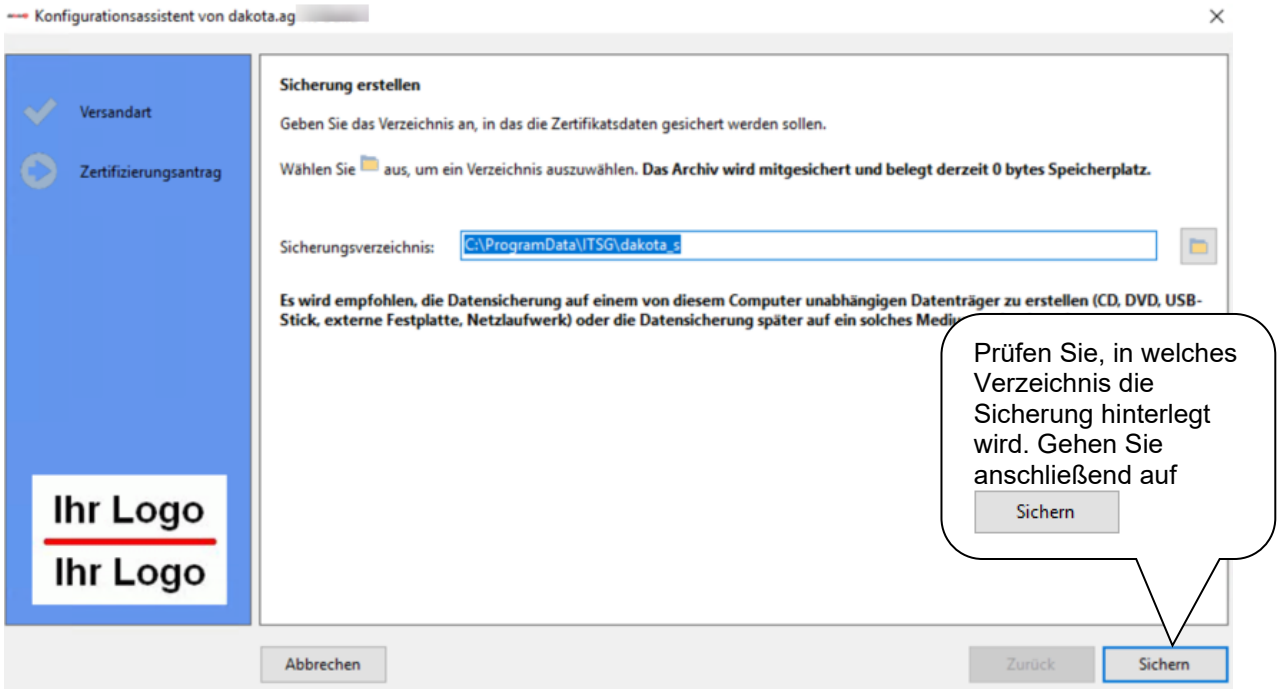


Sollte die Übertragung an das ITSG-Trust Center über das Internet nicht möglich sein, bietet Ihnen dakota an dieser Stelle einen *alternativen* Versandweg per E-Mail an. Dies ist aber nur möglich, wenn Sie, wie unter Punkt 2.3.3.1 beschrieben, ein Ersatzverfahren eingerichtet haben.



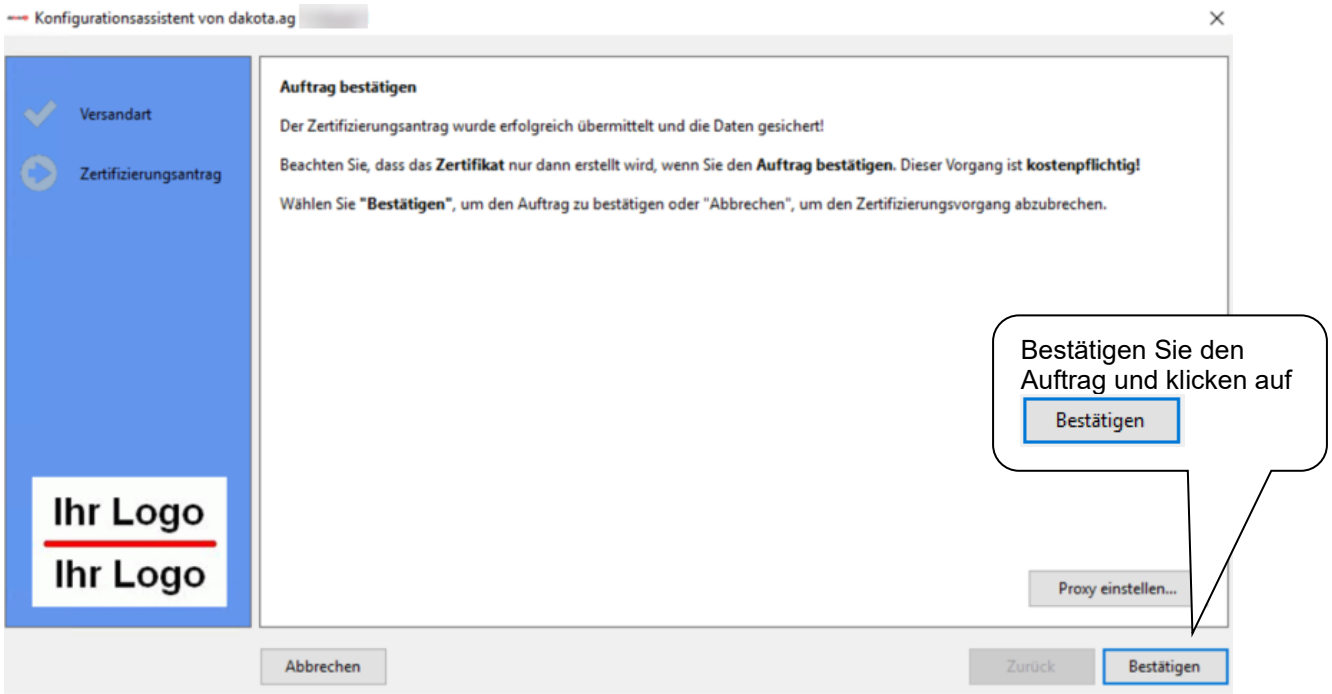
Sobald Ihr Zertifizierungsantrag an das ITSG-Trust Center übertragen wurde, erhalten Sie eine Quittungs-E-Mail. Die Quittung enthält eine Auftragsnummer, mit dieser **Auftragsnummer** können Sie Ihren Antrag auch im Internet verfolgen. Gehen Sie auf die Internetseite www.trustcenter.info und wählen Sie die **Online Antragsverfolgung**. Über die Online Antragsverfolgung können Sie Ihren Schlüssel und alle notwendigen Schlüssel der Datenannahmestellen herunterladen.

dakota erstellt nun für Ihre Schlüsseldaten einen Sicherungsordner.

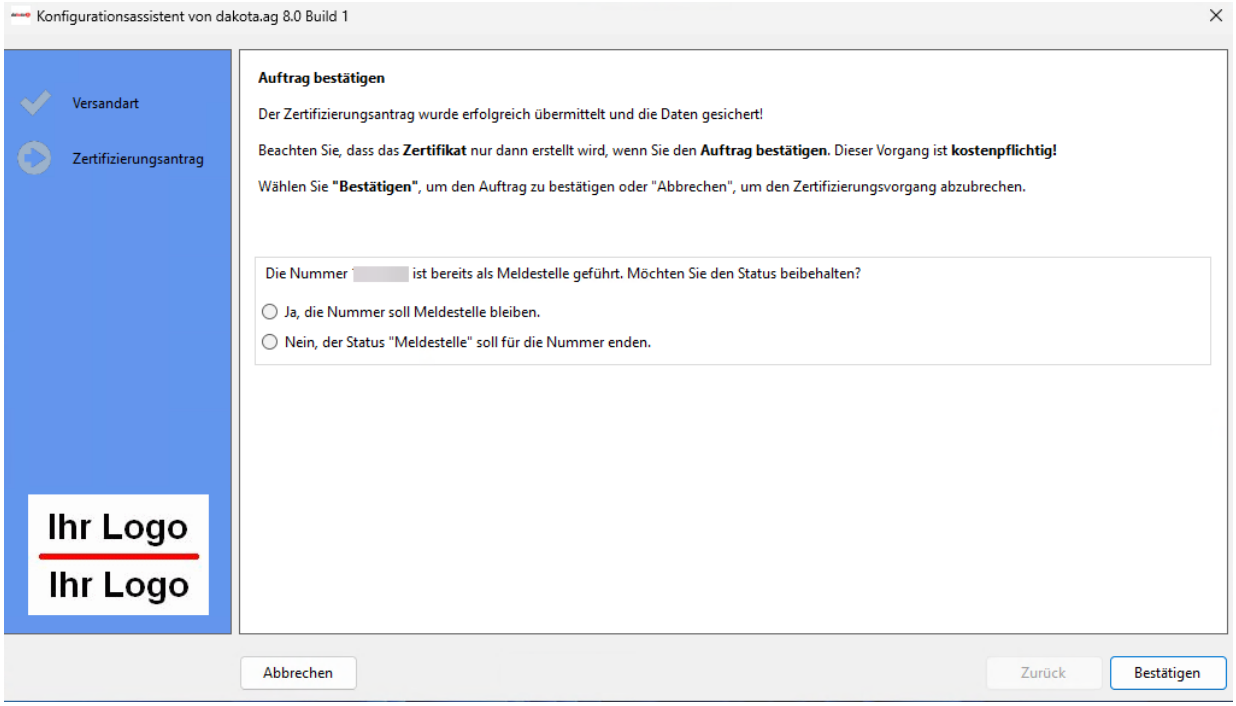


Hinweis: Wenn Sie Ihre Sicherungskopie in einem anderen Verzeichnis als angegeben speichern möchten, klicken Sie bitte auf .

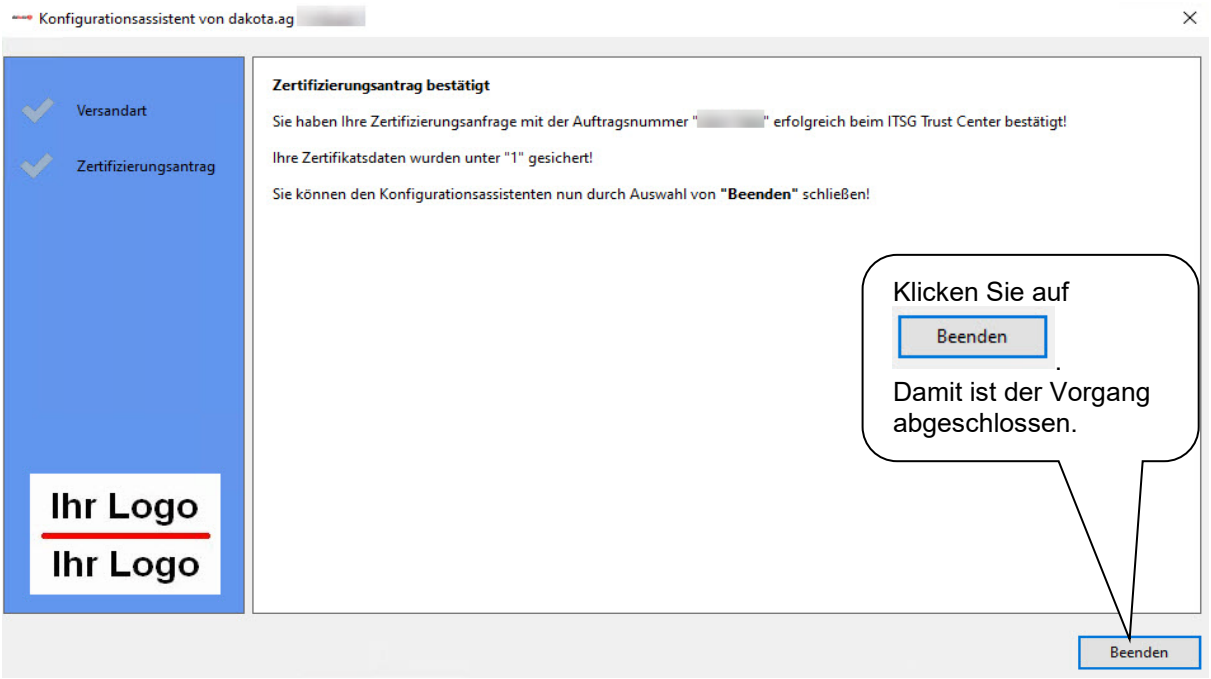
Am Ende des Vorgangs müssen Sie den Zertifizierungsantrag nochmals bestätigen. Erst wenn der Zertifizierungsantrag bestätigt wurde, wird das ITSG-Trust Center den Antrag bearbeiten. Sollte die Bestätigung nicht erfolgen, so wird der Antrag von dakota gelöscht.



Sollte Ihr aktuelles Zertifikat den Status Meldestelle haben, so wird bei einem Folgeantrag abgefragt, ob Sie den Status Meldestelle fortführen oder beenden möchten.
Im gleichen Schritt wird der Antrag mit Ihrer Auswahl bestätigt.



Abschluss Zertifikatsantrag

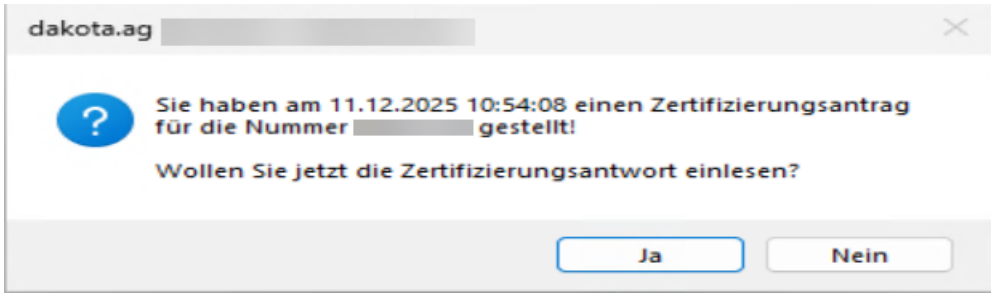


2.3.4.5 Einlesen der Zertifikatsantwort vom ITSG Trust Center

Nach einer Bearbeitungszeit erhalten Sie eine E-Mail vom ITSG-Trust Center mit der Zertifikatsantwort. In dieser E-Mail sind im Anhang Ihre Zertifikatsantwort und die Schlüssel der Datenannahmestellen beigefügt. Zum Einlesen der Zertifikatsantwort bietet Ihnen der Konfigurationsassistent zwei mögliche Verfahren.

Besteht eine Internetverbindung und dakota hat Zugriff darauf, so werden die nachfolgenden Schritte durch dakota automatisch durchgeführt.

Starten Sie dakota. Der Assistent wird mit nachfolgender Maske am Bildschirm erscheinen:



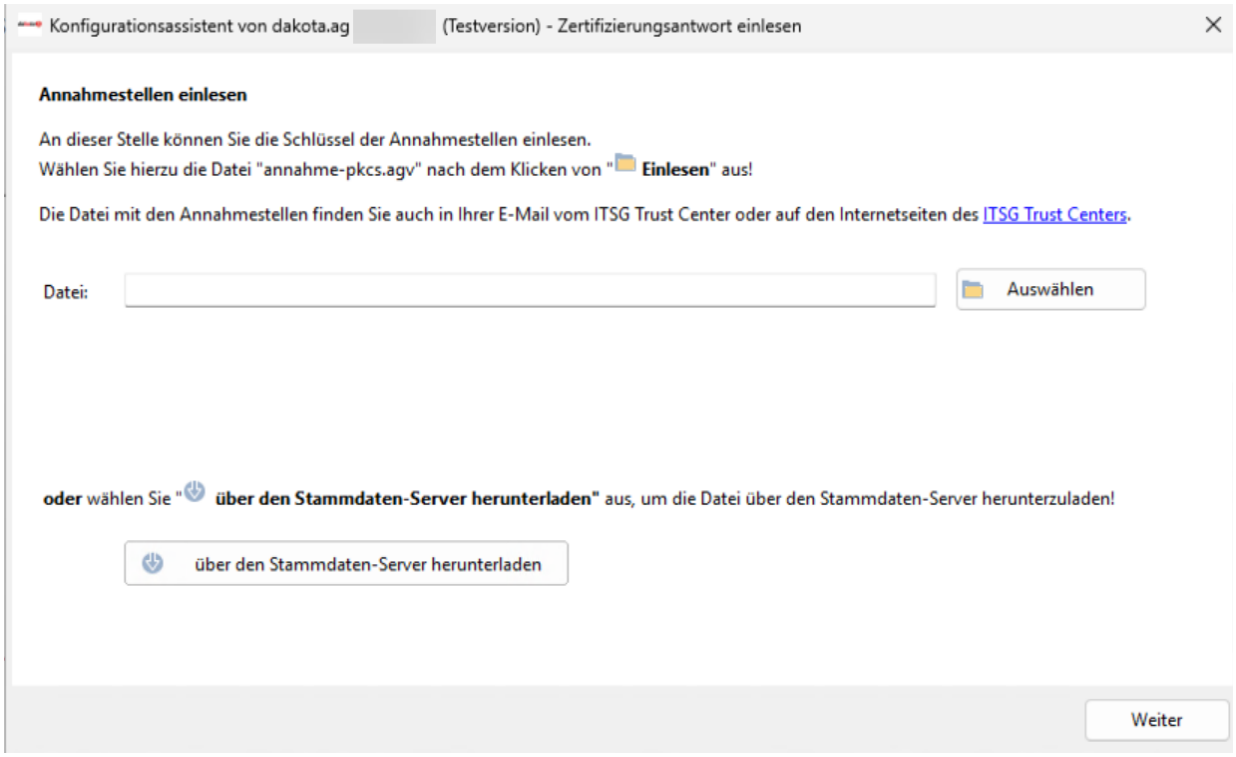
Wählen Sie **Ja**, so geht der Assistent direkt in den Modus **Abholen**.



Sollte das Herunterladen der Zertifikatsantwort scheitern, so kann der Schlüssel aus der E-Mail über einen Speicherort Ihrer lokalen Festplatte eingelesen werden.

Speichern Sie bitte die Dateianhänge der E-Mail auf Ihrer lokalen Festplatte. Wählen Sie im Assistenten den Button und geben Sie den Speicherort der Datei **Zertifizierungsantwort** ein.

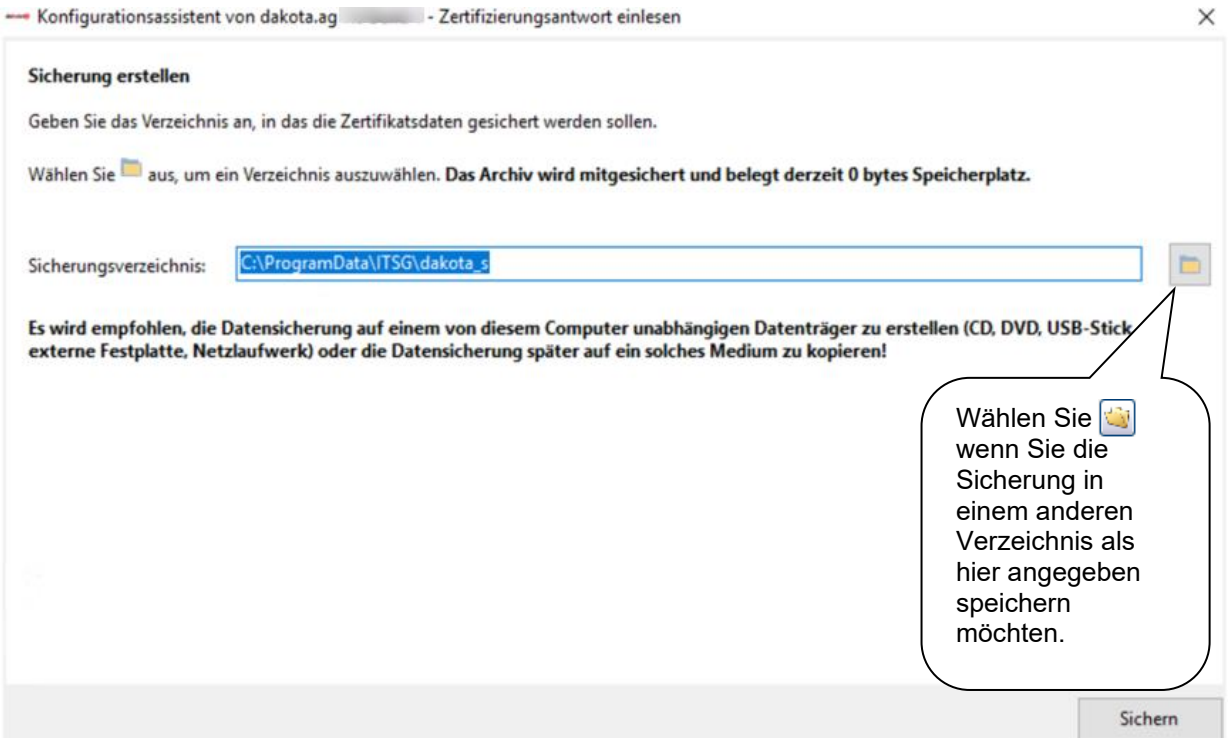
Nun müssen Sie noch die Schlüssel der Datenannahmestellen einlesen. Hierzu verbindet sich dakota automatisch im nächsten Schritt mit dem Stammdatenupdateserver und lädt sich die entsprechenden Dateien herunter.
Sie können die Datei Annahme-pkcs.agv (Arbeitgeberverfahren) oder Annahme-pkcs.key (Leistungserbringerverfahren) auswählen.



Sollte das Herunterladen der Stammdaten scheitern, so kann die Schlüsselliste aus der E-Mail über einen Speicherort Ihrer lokalen Festplatte eingelesen werden.
Wählen Sie hierfür Auswählen und geben Sie den Speicherort der Datei **Annahme-pkcs.agv** oder **Annahme-pkcs.key** ein.

Sie haben nun die Software erfolgreich eingerichtet. Für den Fall, dass Sie dakota neu installieren möchten, benötigen Sie Ihre persönlichen Einstellungen.

Der Konfigurationsassistent bietet Ihnen nun die Möglichkeit Ihren Stand zu sichern. Wählen Sie über ein Verzeichnis, in dem Sie die persönlichen Einstellungen speichern möchten und wählen Sie anschließend Sichern .



Sobald die Sicherung Ihrer persönlichen Daten erfolgreich ausgeführt wurde, erhalten Sie folgende Meldung am Bildschirm:



dakota ist jetzt eingerichtet und bereit Daten zu verarbeiten.

3 Verarbeitung

3.1 Kurzbeschreibung

Nach abgeschlossener Inbetriebnahme Ihres Systems mit dem Assistenten können Sie die von Ihrer Fachanwendung bereitgestellten Dateien mit dakota **verschlüsseln** und an die Annahmestellen der Sozialversicherungsträger **versenden**. Die Fachanwendung erstellt hierfür eine Datei mit den Daten.

Beim Verschlüsseln durchsucht dakota die Übergabeverzeichnisse auf vorhandene Dateien. Diese Dateien werden geprüft und verschlüsselt. Dieser Vorgang wird protokolliert und kann entsprechend über die Detailansicht oder über das Kurzprotokoll geprüft werden. Anschließend werden die Dateien nach Kassenart sortiert in die Unterverzeichnisse der Versandordner geschrieben.

Beim Versenden durchsucht dakota alle Unterverzeichnisse in den Versandordnern auf vorhandene Dateien. In diesem Verzeichnis stehen alle zuvor verschlüsselten Dateien.

Treten Probleme bei der Verarbeitung der Dateien auf, können Sie die Protokolldateien auswerten. Sollten Sie weitere Fragen oder Probleme an dieser Stelle haben, wenden Sie sich an Ihr Softwarehaus um gemeinsam die Protokolldateien auszuwerten. Mehr zu den Protokollinformationen finden Sie im Kapitel 4 Protokollierungen.

Achtung:
Fehlerbehaftete Dateien werden von dakota nicht verarbeitet. Alle fehlerhaft geprüften Dateien bleiben im Übergabeverzeichnis stehen. Die fehlerhaften Daten müssen vor der nächsten Verarbeitung gelöscht werden. Nach einer fehlerfreien Verarbeitung stehen keine Dateien mehr im Übergabeverzeichnis.

3.2 Programmstart

Haben Sie in Ihrer Fachanwendung Meldungsdateien oder Beitragsnachweise erzeugt, die Sie übertragen möchten? In der Regel wird Ihnen Ihr Softwarehaus in Ihre Fachanwendung eine Funktion für 

mit dakota integrieren. Der Name für den Programmaufruf kann hier natürlich von Softwarehaus zu Softwarehaus variieren. Trifft dies für Sie zu, lesen Sie bitte weiter im Kapitel 3.4 Verschlüsseln und Versenden integriert in die Fachanwendung.

Alternativ können durch den direkten Programmstart von dakota Dateien verarbeitet werden.
⇒ Wählen Sie hierfür *'Start → Alle → dakota → dakota...'*.

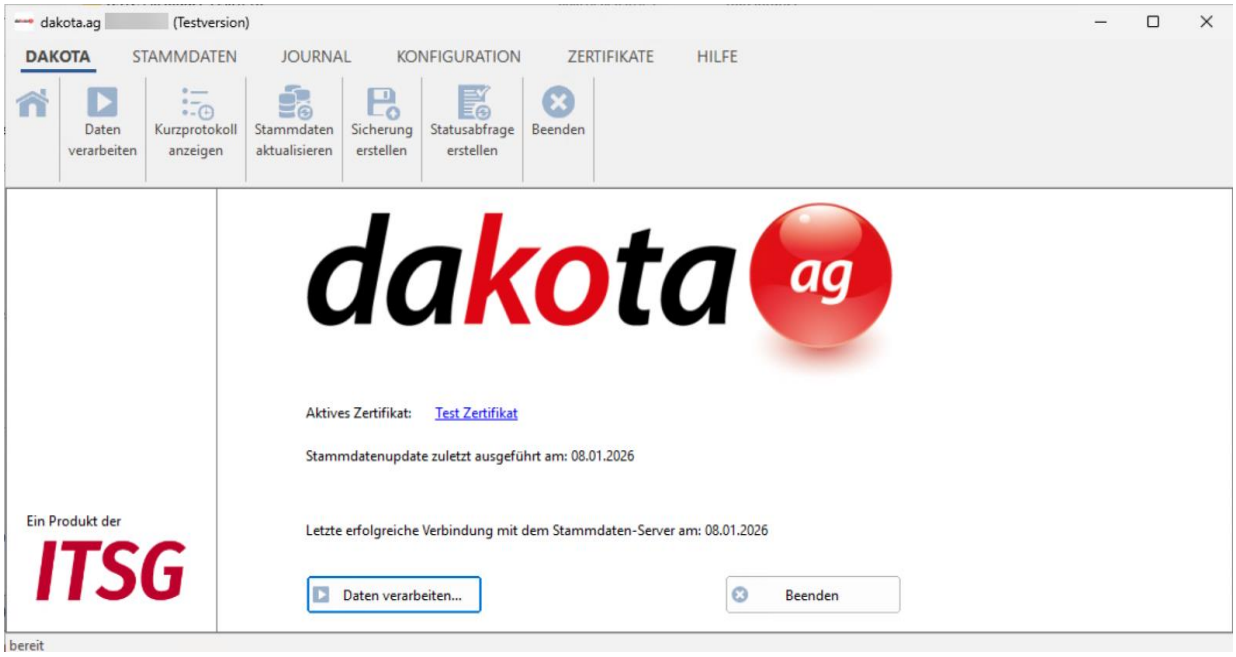


Abbildung dakota.ag

3.3 Daten durch den Direktaufruf von dakota verarbeiten

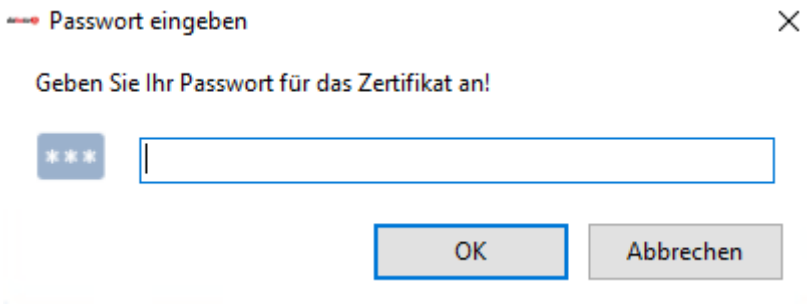
3.3.1 Daten verarbeiten

Beim Verarbeiten der Daten ist es möglich, mit dakota Dateien zu ver- oder entschlüsseln. Für verschlüsselte und unverschlüsselte Daten gibt es getrennte Eingangsverzeichnisse. Bitte beachten Sie das Kapitel 6. Dort wird beschrieben, wie Sie die einzelnen Übergabeverzeichnisse und die Verarbeitungsreihenfolge für Ihre Installation von dakota einrichten.

Um die Verarbeitung von Daten zu beginnen, stellen Sie bitte sicher, dass Dateien in den Übergabeverzeichnissen abgelegt sind. Wählen Sie anschließend bitte auf der Hauptmaske von dakota oder über das Menü **Bearbeiten** die Funktion 

aus.

Beim Verschlüsseln durchsucht dakota - nach der richtigen Passworteingabe - das Verzeichnis*Übergabeverzeichnis* auf vorhandene Dateien.



In der nachfolgenden Maske zeigt Ihnen dakota die gefundenen Dateien, die verarbeitet werden sollen, an. Achten Sie darauf, dass Sie online sind. Wählen Sie 

und die Daten werden übertragen.

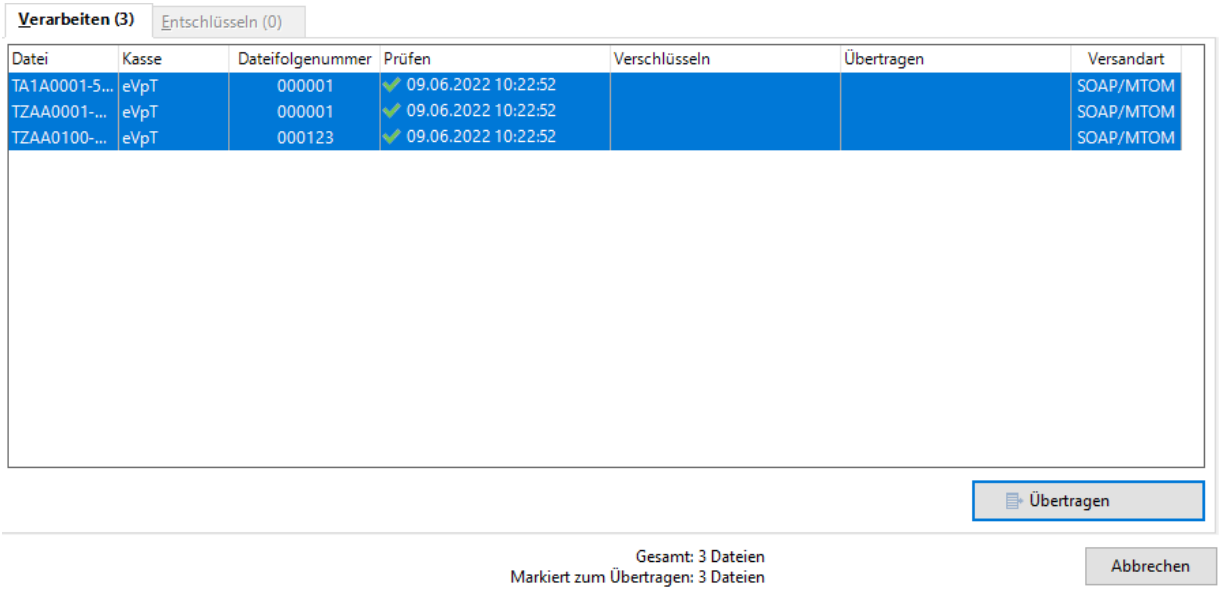


Abbildung dakota.ag

Aus dem Vorlaufsatz der Dateien wird von dakota die Kassenart ermittelt und die erfolgreich geprüfte Datei in das Unterverzeichnis dieser Kassenart in das Verzeichnis *\Versandordner\Name Kassenart* geschrieben und aus dem *\Übergabeverzeichnis* gelöscht. Lediglich fehlerhafte Dateien bleiben im Übergabeverzeichnis stehen und müssen von Ihnen manuell gelöscht werden.

Beachten Sie hier die Fehlermeldung beim Prüfen, Verschlüsseln oder Versenden. Möchten Sie den Vorgang komplett neu starten, weil z. B. die Datei fehlerhaft erzeugt wurde, gehen Sie bitte in das Kurzprotokoll und sehen Sie sich die Details der Verarbeitung an. Das Kurzprotokoll bietet Ihnen umfassende Möglichkeiten zur Administration.

3.3.2 Versenden über *SOAP/MTOM* (nur dakota.ag)

Beachten Sie bitte, dass vor dem Versand die Verbindung zum Internet aktiviert sein muss. Ohne eine Internetverbindung ist der Datenversand nicht möglich.

3.3.3 Versenden per E-Mail: dakota-E-Mail

Beachten Sie bitte, dass bei der Versandart dakota-E-Mail die Verbindung zum Internet aktiviert sein muss. Ohne eine bestehende Internetverbindung findet kein Versand statt.

3.3.4 *Multitenant App Registration im Entra Admin Center* mit OAuth2

1. **Anmelden im Entra Admin Center**

- Melden Sie sich unter entra.microsoft.com mit einem Konto mit Administrationsrechten an.

2. **Neue App-Registrierung anlegen**

- Wählen Sie im linken Menü App-Registrierungen und dann Neue Registrierung.
- Geben Sie einen Namen für Ihre Anwendung ein z.b dakota
- Wählen Sie Konten in jedem Organisationsverzeichnis (beliebiges Azure AD-Verzeichnis – Multimandanten).
- Tragen Sie unter Umleitungs-URI Ihre gewünschten URIs ein:
  - Select a platform
  - Public Client / Native (mobile & Desktop)
  - http://localhost/
  - https://login.microsoftonline.com/common/oauth2/nativeclient

3. **API-Berechtigungen hinzufügen**

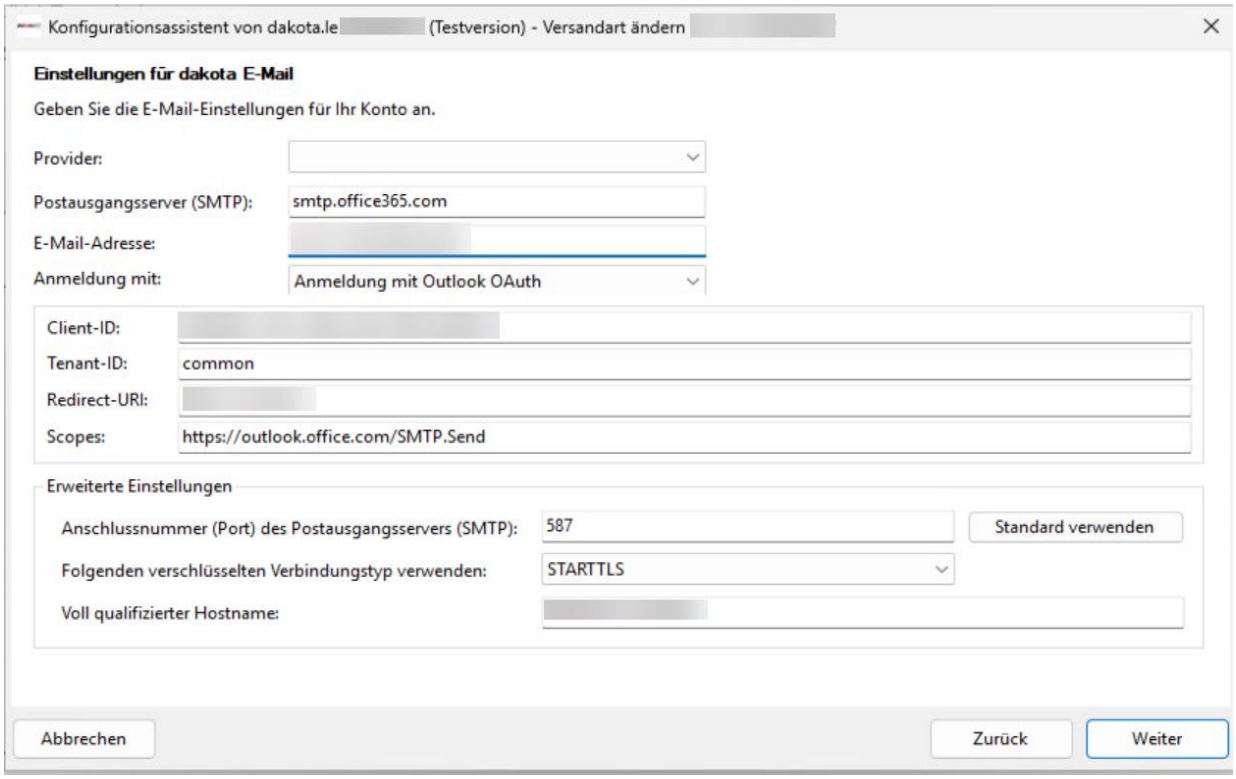
- Wechseln Sie zur neu angelegten App-Registrierung.
- Wählen Sie im Menü API-Berechtigungen > Berechtigung hinzufügen.
- Wählen Sie Microsoft Graph.
- Fügen Sie unter Anwendungsberechtigungen die Berechtigung SMTP.Send hinzu.
- Fügen Sie unter Berechtigungen im Delegiert-Modus die Berechtigung User.Read hinzu.
- Klicken Sie auf Berechtigungen hinzufügen.
- Admin-Konsens erteilen, damit die App die Berechtigungen nutzen kann.

4. **Folgende Informationen für die dakota Konfiguration notieren**

- Anwendungs-ID (Client-ID)
- Verzeichnis-ID (Tenant-ID) finden Sie auf der Übersichtsseite der App-Registrierung.
- Die Umleitungs-URIs müssen auch in Ihrer Anwendungskonfiguration(dakota) hinterlegt werden.

Folgende Daten sind zu verwenden:

- Postausgangsserver smtp.office365.com
- Zu Verwendende E-Mail Adresse
- Notierte Daten aus dem Entra Admin Center (Client, Tenant, Redirect URI)
- Scopes https://outlook.office.com/SMTP.Send
- Port 587 und STARTTLS als verschlüsselten Verbindungstyp



3.3.5 Versenden über die Verzeichnis-Ausgabe

Haben Sie bei der Konfiguration der Versandart die Option **<Verzeichnis-Ausgabe>** gewählt, werden die verschlüsselten Dateien in einem Unterordner mit Tagesdatum und Uhrzeit abgelegt.

Bei dakota.le wird zusätzlich eine Informationsdatei abgelegt. Die Auftragssatzdatei muss jeder verschlüsselten Datei beigefügt werden und dient der genauen Adressierung der verschlüsselten Nutzdaten. Die Informationsdatei enthält alle notwendigen Angaben zum Versand der jeweiligen verschlüsselten Nachricht.

Bei dakota.ag wird im Ausgabeverzeichnis eine XML-Datei hinterlegt. Diese XML-Datei enthält die Informationen über den Empfänger sowie die verschlüsselte Datei, welche an die Kommunikationsserver oder an die Datenstelle übertragen werden muss.

Achtung:
Es gibt derzeit keinen vorgegebenen Weg, außer über die Kommunikationsserver, eine Meldung in einer XML-Datei an die Datenstellen zu übertragen.

3.4 Verschlüsseln und Versenden integriert in die Fachanwendung

Der so genannte Execute-Modus von dakota bietet den Softwarehäusern die Möglichkeit, die Funktionalität von dakota über parametergesteuerte Aufrufe in die eigene Fachanwendung zu integrieren. So kann die komplette Verarbeitung (Verschlüsseln und Versenden), der Aufruf des Assistenten und die Anzeige der Kurzprotokolle von Ihrer Fachanwendung aufgerufen und gesteuert werden.

Sie werden dann aus Ihrer Fachanwendung Statusmeldungen, wie z. B. *"Verarbeitung erfolgreich durchgeführt"* oder *"Fehler beim Verschlüsseln/Versenden der Datei xy",* zur dakota-Verarbeitung erhalten. Gegebenenfalls wird Ihnen bei einer fehlerhaften Verarbeitung das Kurzprotokoll zur Fehleranalyse sofort angezeigt oder kann von Ihnen über den Assistenten unter **<Kurzprotokoll>** aufgerufen werden. Der Integrationsgrad von dakota kann natürlich von Softwarehaus zu Softwarehaus variieren.

Bei aufgetretenen Fehlern beim Verschlüsseln oder Versenden wird Ihnen im Kurzprotokoll die Verarbeitungszeile in roter Schrift angezeigt. Markieren Sie die gewünschte Zeile und wählen Sie dann Details anzeigen.

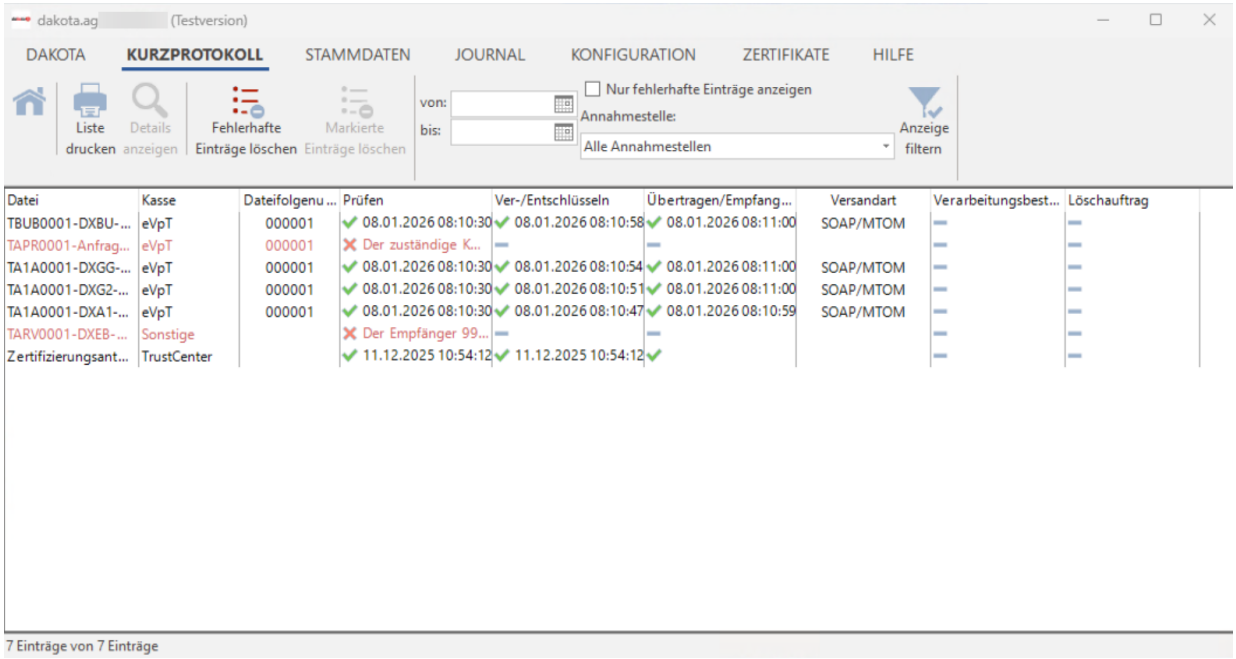


Abbildung dakota.ag

Wurden Dateien fehlerfrei verschlüsselt, konnten aber im Execute-Modus nicht versendet werden, können Sie den Sendevorgang für diese Dateien mit **<Daten verarbeiten>** erneut starten.

Weitere Informationen zur Auswertung des Kurzprotokolls finden Sie im Kapitel 4 Protokollierung.

4 Protokollierung

4.1 Kurzbeschreibung

dakota erzeugt mehrere Arten von Protokolldateien. So werden für alle Annahmestellen separate Logdateien geführt. Die Schlüsselgenerierung des Endanwenders wird ebenfalls in einer Logdatei festgehalten und dakota schreibt eine Aufruf-Logdatei. Diese Logdateien werden **Langprotokolle** genannt und sind für die Abstimmung mit Ihrem Softwaresupport gedacht. Zusätzlich werden alle dakota-Verarbeitungsschritte für den Endanwender als **Kurzprotokoll** aufgelistet. Diesen Kurzprotokollen kann der aktuelle Bearbeitungsstatus und evtl. aufgetretene Fehler bei der Verarbeitung von Dateien entnommen und ggf. gemeinsam mit dem Softwaresupport analysiert werden. Über die Detailansicht einer Datei im Kurzprotokoll kann ein Neuversand angestoßen werden.

4.2 Langprotokoll

Wenn für eine Annahmestelle das erste Mal Meldungen geprüft und verschlüsselt werden, so wird ein Langprotokoll als Logdatei angelegt. Diese Datei wird nur einmal angelegt und weiter fortgeschrieben. Sobald die Datei eine bestimmte Größe erreicht hat, werden die alten Daten rollierend überschrieben. Die Größe kann unter Konfiguration -> Einstellungen festgelegt werden. Die Logdatei beinhaltet Meldungen der Prüfung und der Verschlüsselung, wann und mit welchem Ergebnis die Daten für diese Annahmestelle bearbeitet wurden. Sie finden alle Logdateien im Standardpfad *C:\dakota\proto*. Pro Annahmestelle wird eine Logdatei mit dem Dateinamen *Betriebsnummer.log* bzw. *IK-Nummer.log* erstellt.

Für den Anwender wird, sobald er seinen privaten Schlüssel generiert, ebenfalls eine Protokolldatei angelegt - erstmalig bei der Inbetriebnahme. Hierin können bei Bedarf Probleme bei der Schlüsselgenerierung analysiert werden.

dakota dokumentiert seine einzelnen Aufrufe mit den Parametern im Execute-Modus. Die einzelnen Funktionen innerhalb des Verarbeitungslaufes werden ebenfalls zu Analysezwecken in diese rollierende Logdatei aufgenommen. Die Datei trägt die Bezeichnung *dakota.log*.

4.3 Kurzprotokoll

Im Kurzprotokoll wird für jeden Verarbeitungsschritt ein Protokolleintrag erstellt. Diesem können Sie entnehmen welche Dateien von dakota wie und wann verarbeitet wurden.

⇒ Starten Sie dakota und wählen Sie aus dem Hauptmenü *'Datei → Kurzprotokoll'*

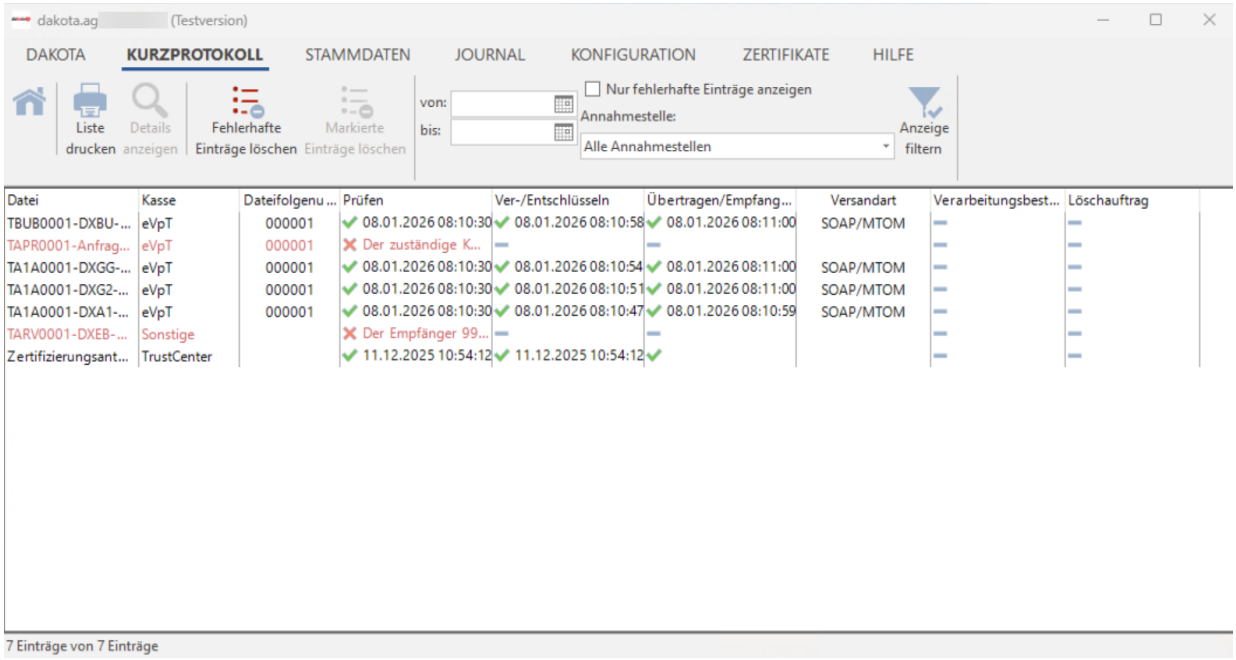


Abbildung dakota.ag

Durch einen Klick auf Spaltenbezeichnung lässt sich das Kurzprotokoll sortieren.

Sie können die Anzeige der Einträge nach **Datum** oder **Annahmestelle** filtern. Tragen Sie den gewünschten Zeitraum in die Felder *„von:“ „bis:“* ein und wählen **Anzeige filtern.** Dann erhalten Sie alle vorliegenden Daten in diesem Zeitraum. Möchten Sie alle Daten einer Annahmestelle filtern, wählen Sie diese aus der Empfängerliste aus und wählen **Anzeige filtern**.
Mit einem Doppelklick in eine fehlerfrei versendete Zeile erhalten Sie die Detailansicht.

4.3.1 Detailansicht

Die Detailansicht bietet Ihnen mehrere Möglichkeiten der Administration Ihrer versendeten Nachrichten. Sie können die folgenden Funktionen auf der Detailansicht auswählen:

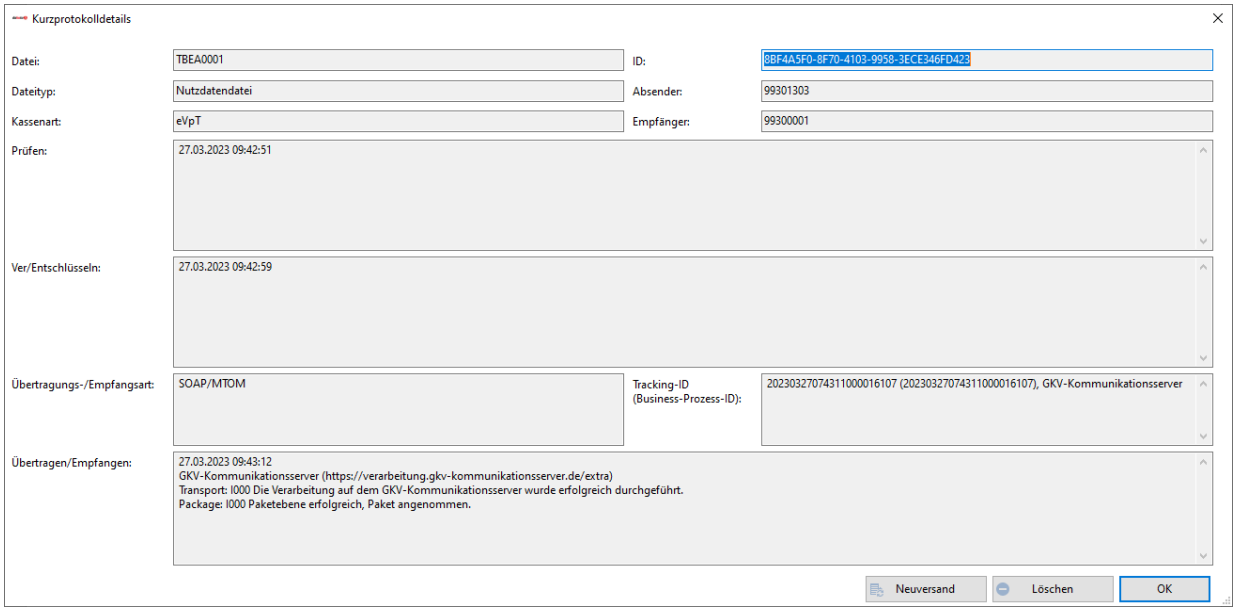


Abbildung dakota.ag

- **Löschen**
  Wenn bei der Verarbeitung Fehler auftreten, werden diese Zeilen rot markiert. Die Funktion 

bietet Ihnen die Möglichkeit, die fehlerhafte Datei zu löschen. Die fehlerhafte Datei wird aus dem Verzeichnis entfernt und das Kurzprotokoll aktualisiert.

- **Neuversand**
  Die Funktion 

steht Ihnen nur bei der Versandart **Kommunikationsserver** oder **dakota-E-Mail** zur Verfügung. Beim Neuversand wird eine Kopie der bereits gesendeten Daten aus dem Archiv verwendet und erneut an die Annahmestelle gesendet. Der Neuversand kann nur bei erfolgreich gesendeten Dateien ausgewählt werden. Bei der Versandart Verzeichnisausgabe steht Ihnen der Neuversand nicht zur Verfügung.

5 dakota-Aktualisierung

5.1 Kurzbeschreibung

Nach abgeschlossener Inbetriebnahme stellt Ihnen der dakota-Assistent bzw. das dakota–Hauptmenü weitere Funktionen zur Konfiguration zur Verfügung. Da Ihr eigenes Zertifikat und die Schlüssel Ihrer Annahmestellen nur eine begrenzte Laufzeit haben, stellt Ihnen der dakota-Assistent hier die erforderlichen Funktionen zur Aktualisierung Ihres Schlüssels bzw. zum erneuten Einlesen der Schlüssel Ihrer Annahmestellen bereit. Sollte Ihr Zertifikat defekt oder ‚unsicher' geworden sein oder sich der verantwortliche Ansprechpartner in Ihrer Firma ändern, können Sie über den Assistenten einen neuen Schlüssel generieren und damit ein neues Zertifikat beantragen (siehe unter *„Neues Zertifikat"*).

Die Aktualisierung Ihrer **Annahmestellen** ist ebenso möglich, wenn diese z. B. durch das Entstehen einer neuen Annahmestelle nötig ist. Öffnen Sie das Menü **<Stammdaten>** und wählen Sie die Funktion **<Stammdaten aktualisieren>** und anschließend



aus. Die Software holt alle notwendigen Informationen automatisch aus dem Internet ab und importiert sie. Wir empfehlen Ihnen, vor und nach jeder Aktualisierung eine Sicherung Ihrer Software anzufertigen. Nutzen Sie hierfür die Funktion **<Sicherung erstellen>**. Diese Funktion finden Sie über das Menü **<Zertifikate>**.

5.2 Neues Zertifikat

Ihre Stammdaten für den Zertifizierungsantrag und Ihr Schlüssel werden erstmalig bei der Inbetriebnahme vor der Schlüsselgenerierung von Ihnen erfasst bzw. von Ihrem Anwendungsprogramm übergeben. Die eigenen Stammdaten werden zum einen für die Generierung des Schlüssels und für die Zertifizierung benötigt. Zum anderen werden Stammdaten für die Verarbeitung und die Kommunikation / Versandart festgelegt.

Sofern Sie bereits ein Zertifikat besitzen, prüfen Sie bitte, ob einer der nachfolgenden Punkte zutrifft, bevor Sie einen neuen Schlüssel generieren:

- Ist Ihr Zertifikat defekt und von Ihnen nicht (mehr) rekonstruierbar (z. B. durch eine Sicherung)?
- Haben Sie den Verdacht, dass Ihr Zertifikat „unsicher" geworden ist, d. h. dass ein Unbefugter evtl. Kenntnis hiervon erlangt hat?
- Läuft Ihr Zertifikat in Kürze aus und Sie möchten Ihr Zertifikat beim ITSG Trust Center verlängern?

Dann generieren Sie mit dieser Funktion einen neuen privaten Schlüssel.

Sie erreichen die Funktion <**Neues Zertifikat**> zur Erzeugung eines neuen privaten Schlüssels nach abgeschlossener Inbetriebnahme im Assistenten.

Gehen Sie wie folgt vor:

⇒ Starten Sie den **Assistenten** aus Ihrem Anwendungsprogramm oder alternativ aus dem dakota-Hauptmenü **<Zertifikat>**.

⇒ Wählen Sie **<Neues Zertifikat beantragen>**.

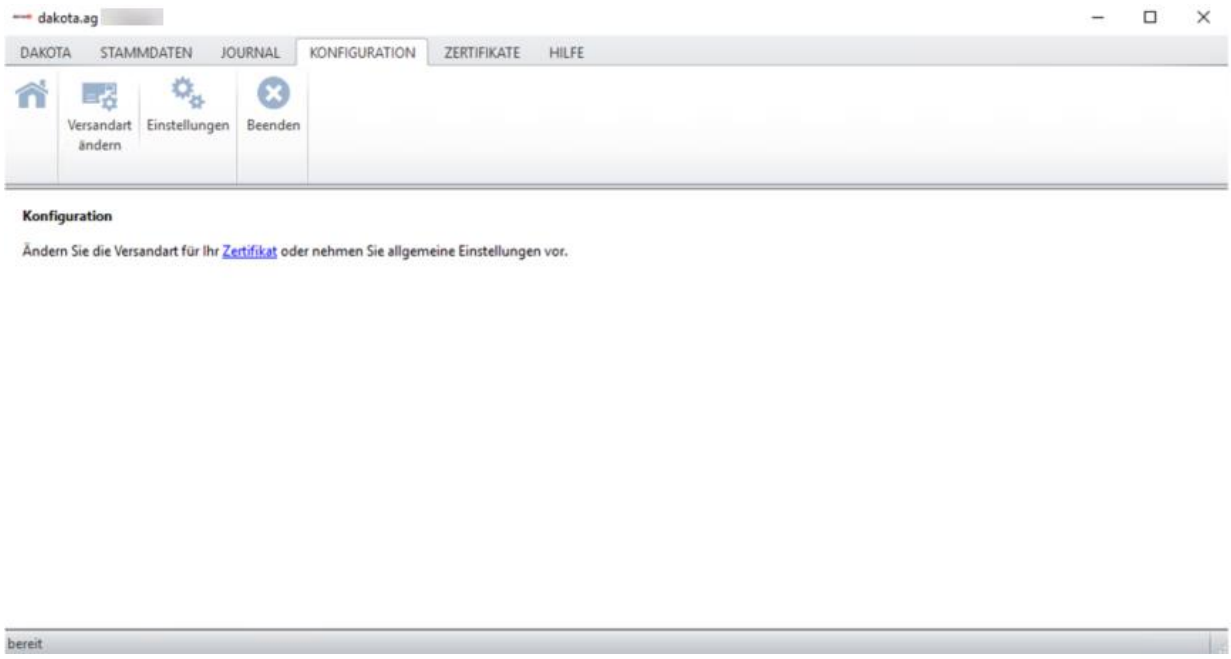
⇒ Wählen Sie nun, ob Sie einen Folgeantrag für das vorhandene Zertifikat oder für eine andere Betriebsnummer bzw. IK-Nummer beantragen wollen.

Anschließend unterstützt Sie der Assistent bei der Eingabe aller notwendigen Daten.

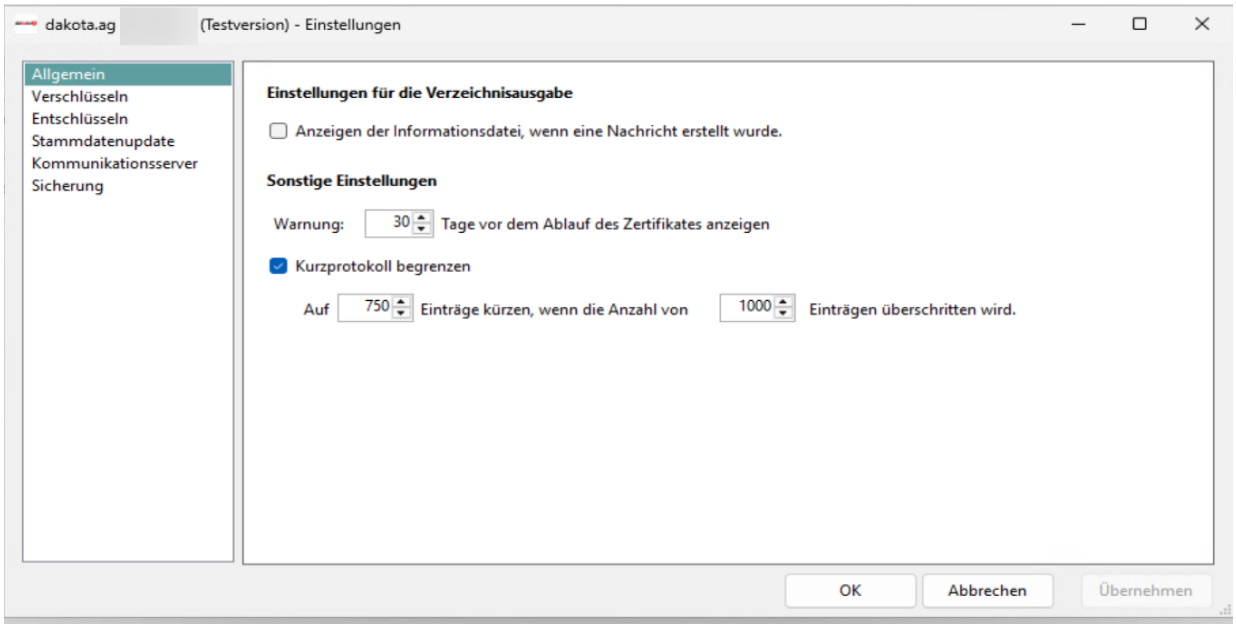
6 Konfiguration

Die dakota-Software bietet Ihnen unterschiedliche Programm-Optionen. Im Folgenden werden die einzelnen Programmoptionen erläutert.

Das Menü **<Konfiguration>** erreichen Sie über die Hauptmaske. Wählen Sie nun bitte **<Einstellungen>**. Die folgenden Optionen stehen Ihnen dort zur Verfügung:



6.1 Allgemeine Einstellungen



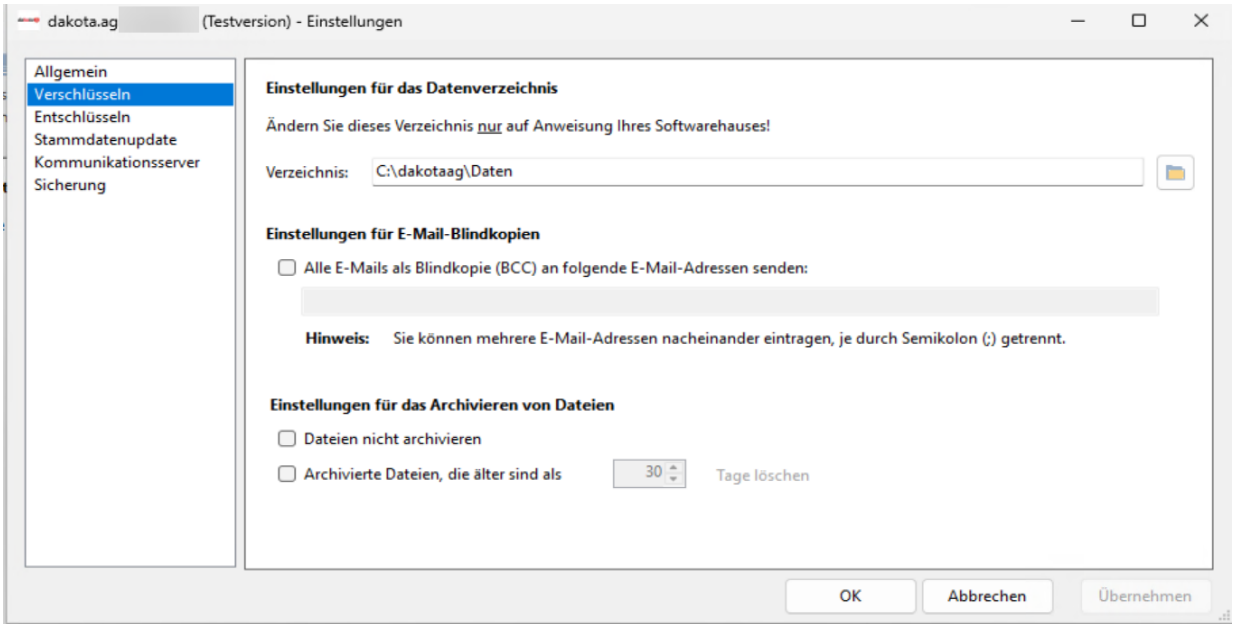
- **Warnung X Tage vor Ablauf des Zertifikates ausgeben.**
  Diese Option informiert Sie über das Ablaufen Ihres Zertifikates. Standardmäßig ist diese Frist auf 30 Tage eingestellt. Ihr Zertifikat vom ITSG-Trust Center ist in der Regel drei Jahre gültig. Der Assistent wird bei jedem Programmstart prüfen, wie lange Ihr Zertifikat noch gültig ist und Sie mit einer Hinweismeldung am Bildschirm informieren, wenn der gewählte Zeitraum für die Warnung erreicht ist. Wenn Ihr Zertifikat abgelaufen ist, müssen Sie einen neuen Zertifizierungsantrag generieren. Lesen Sie hierzu im Kapitel 5.2 Neues weiter.

- **Anzeige der Informationsdateien beim Versand als Verzeichnisausgabe**
  Bei der Versandart Verzeichnisausgabe können Sie sich die Informationsdatei direkt beim Erstellen am Bildschirm anzeigen lassen. In dieser Informationsdatei wird z. B. die E-Mail-Adresse der Annahmestelle abgelegt. Diese Option ist nicht verfügbar, wenn Sie die Versandart Verzeichnisausgabe **nicht** benutzen.

- **Kurzprotokoll begrenzen**
  An dieser Stelle kann festgelegt werden, wie viele Einträge das Kurzprotokoll maximal enthalten darf und auf wie viele Einträge das Kurzprotokoll, bei Erreichen des Limits, gekürzt werden soll. Diese Funktion kann auch deaktiviert werden, sodass keine Einträge gelöscht werden.

6.2 Einstellungen für die Verschlüsselung

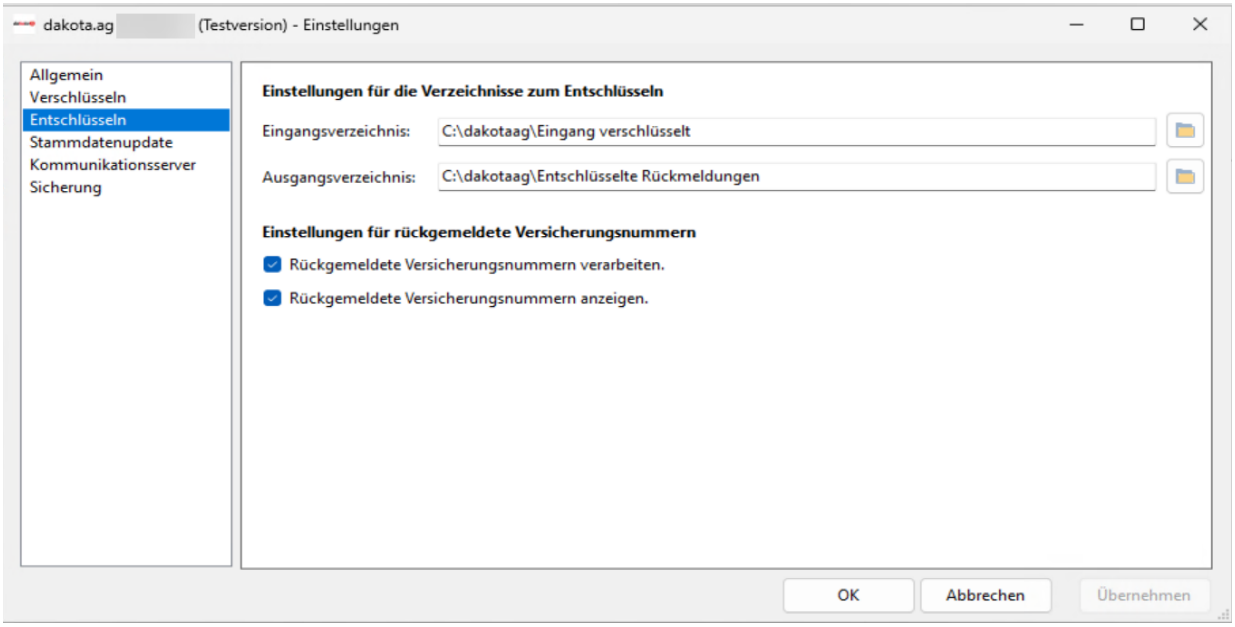
- **Datenverzeichnis**
  Im Datenverzeichnis sucht dakota nach den Abrechnungsdateien, um sie zu verschlüsseln und zu versenden. Wenn Sie den Pfad ändern möchten, können Sie dies über diesen Dialog tun. Um die Pfadangabe zu ändern, wählen Sie bitte



Ebenfalls haben Sie hier die Möglichkeit, zusätzliche E-Mail-Empfänger festzulegen, die Ihre verschlüsselten Daten in Blindkopie (BCC) erhalten sollen.

*BCC-Empfänger werden nicht im Header der E-Mail aufgeführt. Weder beim Hauptempfänger noch bei BCC-Empfängern erscheint ein Hinweis, dass eine BCC gesendet wurde.

6.3 Einstellungen für die Entschlüsselung

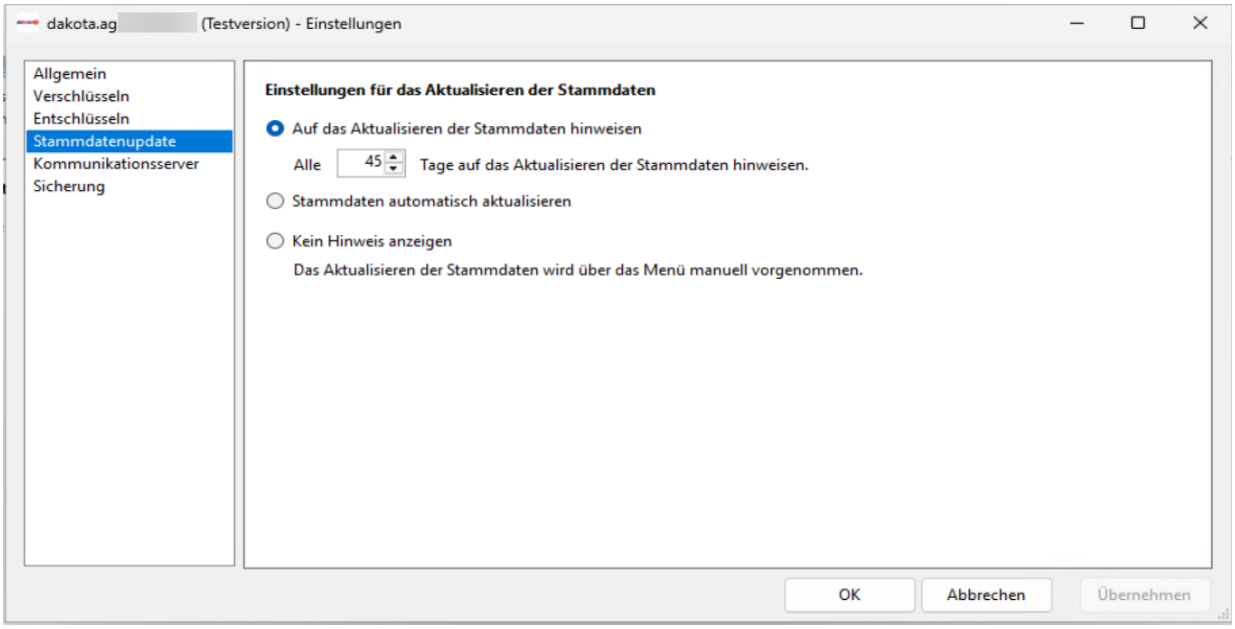


- **Eingangsverzeichnis**
  Im Eingangsverzeichnis sucht dakota nach verschlüsselten Dateien, um sie zu entschlüsseln. Wenn Sie den Pfad ändern möchten, können Sie dies über diesen Dialog tun. Um die Verzeichnisangabe zu ändern, wählen Sie bitte

- **Ausgangsverzeichnis**
  Im Ausgangverzeichnis speichert dakota die entschlüsselten Dateien nach erfolgreicher Entschlüsselung ab. Wenn Sie den Pfad ändern möchten, können Sie dies über diesen Dialog tun. Um die Verzeichnisangabe zu ändern, wählen Sie bitte

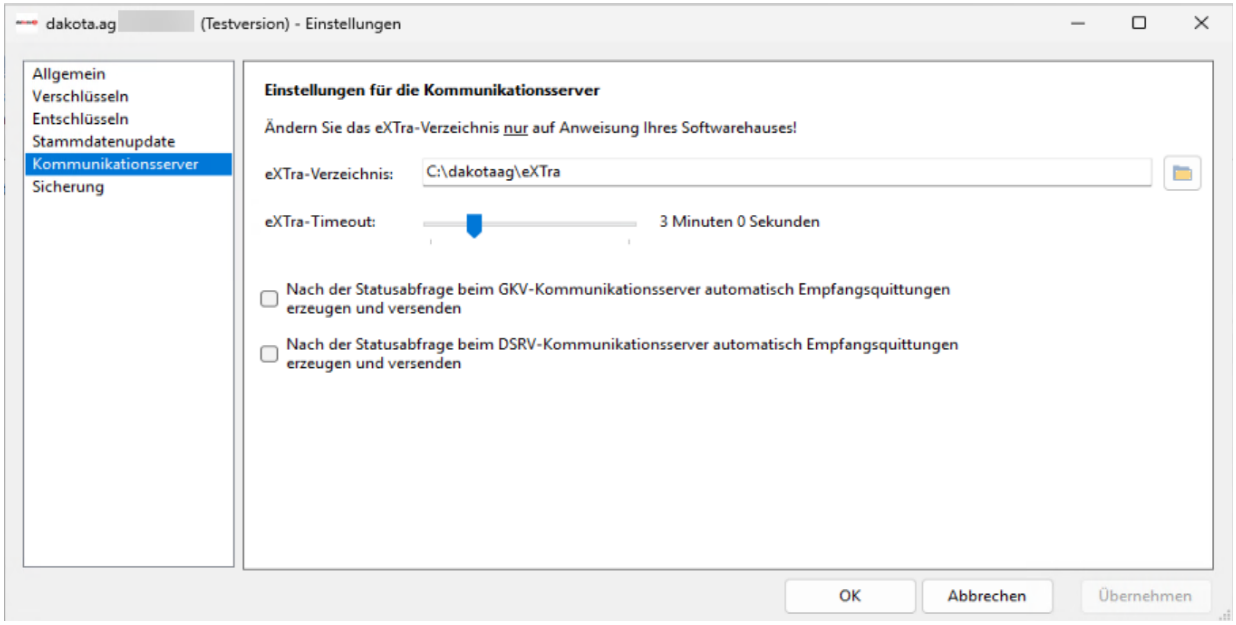
6.4 Einstellungen für das Stammdatenupdate

dakota erinnert Sie regelmäßig an die Aktualisierung der Stammdaten der Annahmestellen. Wenn Sie das Update manuell vornehmen möchten und keine Erinnerung wünschen, können Sie die Erinnerungsfunktion abschalten.



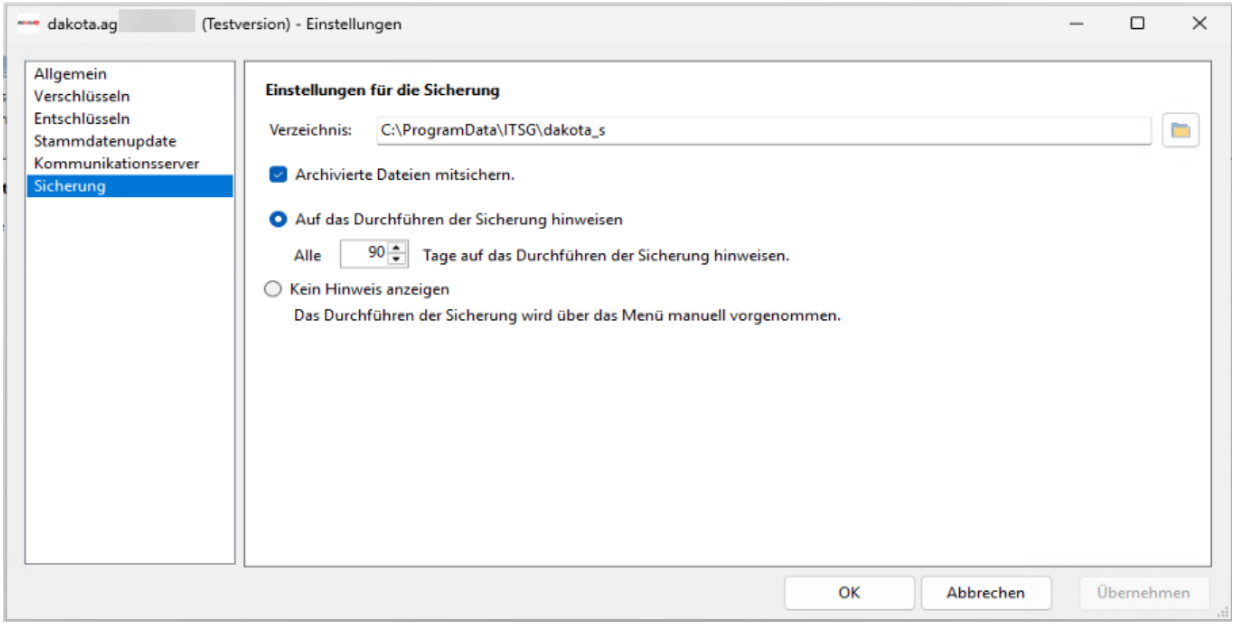
6.5 Einstellungen für den Kommunikationsserver (nur in dakota.ag)

dakota.ag bricht die Verbindung mit dem Kommunikationsserver nach drei Minuten ab, wenn keine Reaktion erfolgt. An dieser Stelle kann der Timeout von dakota.ag zu den Kommunikationsservern erhöht werden.



6.6 Einstellungen für die Schlüsselsicherung

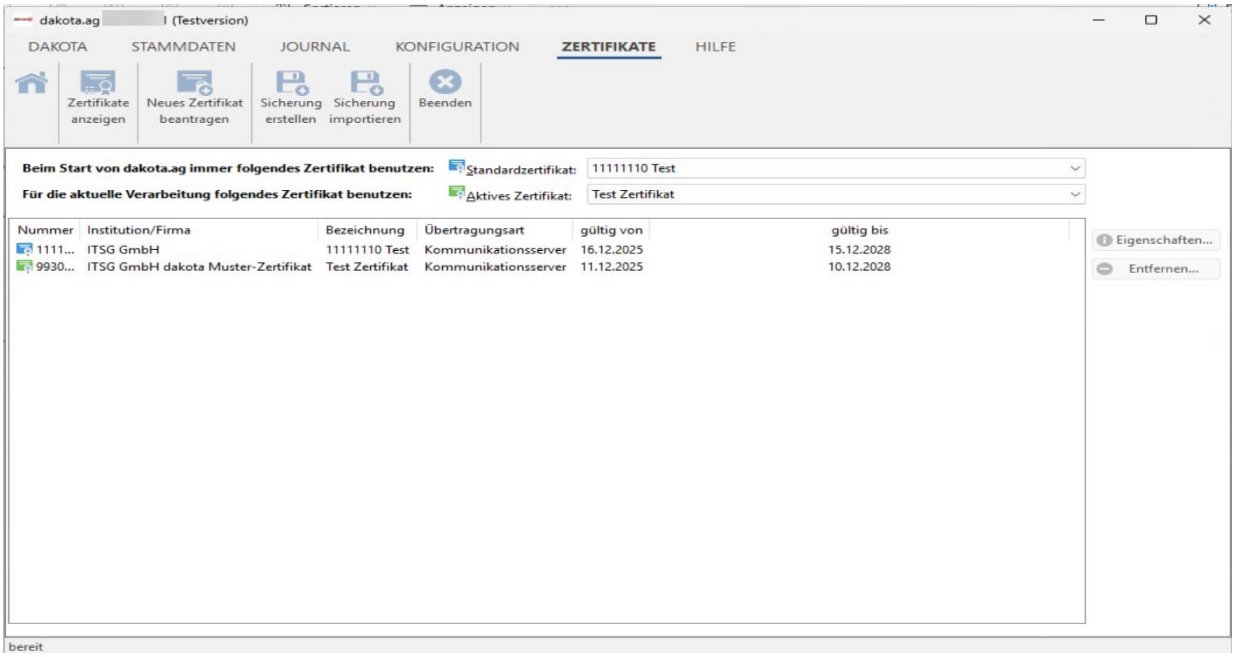
dakota.ag speichert die Sicherung in das Verzeichnis *C:\ProgramData\ITSG\dakota_s bei dakota.le* und in das Verzeichnis *C:\ProgramData\ITSG\dakota_le*. An dieser Stelle kann das Sicherungsverzeichnis angepasst werden. Ebenfalls kann festgelegt werden, ob das Versandverzeichnis von dakota jedes Mal mitgesichert wird.



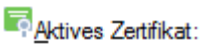
6.7 Zertifikatsverwaltung

Mithilfe der Zertifikatsverwaltung können Sie Ihre Schlüssel in dakota verwalten.

Über den Menüpunkt **<Zertifikate>** erreichen Sie das Menü.

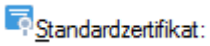


Um ein Zertifikat nur für die laufende Sitzung zu wechseln, gehen Sie über den Menüpunkt



und wählen Sie bitte das Zertifikat für die Sitzung aus.

Über den Menüpunkt



können Sie das Standard-Zertifikat, welches automatisch bei jedem Programmstart gewählt wird, festlegen.

Über die Funktion **<Neues Zertifikat beantragen>** können Sie ein neues Zertifikat beantragen. Wenn Sie bereits bestehende Zertifikate hinzufügen möchten, verwenden Sie bitte die Funktion **<Sicherung importieren>**. Lesen Sie hierzu im Kapitel 6.9 Sicherung importieren.

Bitte beachten Sie: Sie benötigen pro Betriebsnummer immer nur ein Zertifikat. Bei Abrechnungen für mehrere Betriebsnummern erstellen Sie nur für die Betriebsnummer des Abrechnungsbetriebes (für diesen Betrieb ist auch die Zulassung zur DEÜV erfolgt) einen Schlüssel und versenden damit die kompletten Daten. Bei der Verschlüsselung handelt es sich um eine Transportsicherung, die keine Aussagen über den Inhalt trifft. Es genügt lediglich ein Zertifikat für Sie als "versendende Stelle" zu beantragen.

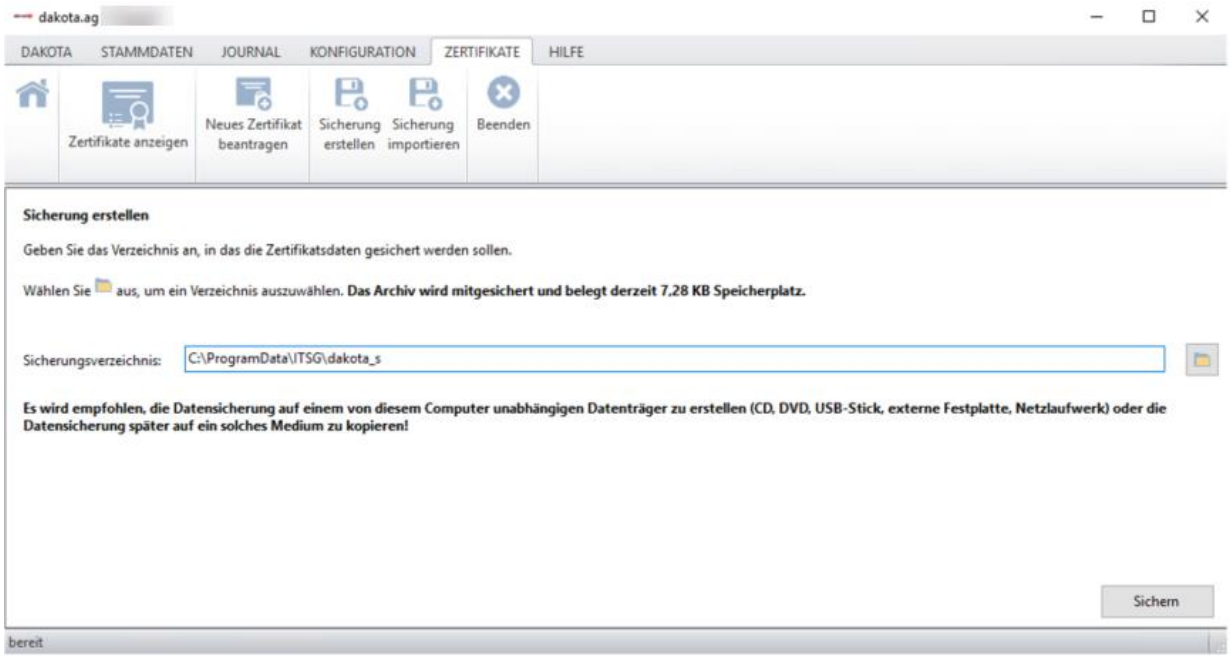
Über 

können Sie nicht mehr benötigte oder abgelaufene Zertifikate entfernen.
Bitte beachten Sie: Wenn Sie ein Zertifikat entfernen, können Sie dies ausschließlich über die Funktion **<Sicherung importieren>** wieder in der Zertifikatsverwaltung hinzufügen.

6.8 Sicherung erstellen

Die dakota-Software bietet Ihnen die Möglichkeit, den aktuellen Stand Ihrer persönlichen Einstellungen zu speichern. Bei Datenverlust können Sie mit dieser Sicherung den vorherigen Stand wiederherstellen. Wir empfehlen Ihnen, in regelmäßigen Abständen Sicherungen anzufertigen und nicht auf der lokalen Festplatte abzulegen. Nutzen Sie zum Beispiel einen USB-Stick, eine externe Festplatte oder einen anderen Datenträger, um Ihre Daten extern zu sichern.

Um eine Sicherung zu erstellen, wählen Sie bitte über die Hauptmaske von dakota das Menü **<Zertifikate> <Sicherung erstellen>**. Der Assistent von dakota wird mit der folgenden Ansicht gestartet:



Wählen Sie über die Funktion ein Verzeichnis, in dem Sie die persönlichen Einstellungen speichern möchten und wählen Sie anschließend Sichern

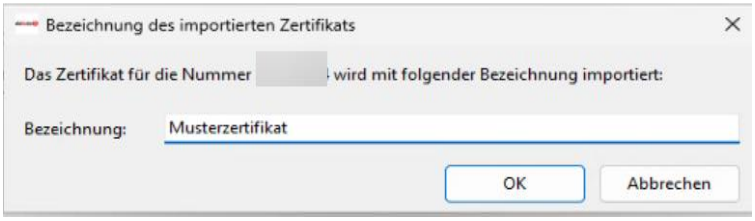
Die Sicherung wird in dem gewünschten Verzeichnis abgelegt. Diese Sicherungsdatei enthält in der Bezeichnung den Zertifikatsstatus, das Tagesdatum und die Betriebsnummer/IK-Nummer.

6.9 Sicherung importieren

Die Software dakota bietet Ihnen die Möglichkeit, eine Sicherung Ihres Schlüssels zu importieren. Falls Sie die Zertifikatsdaten gerne auf ein anderes Computersystem übertragen oder wegen eines Problems im Betriebssystem die Software erneut installieren möchten, können Sie jederzeit eine Sicherung Ihrer Zertifikatsdaten einlesen.

Die Funktion **<Sicherung importieren>** erreichen Sie über die Hauptmaske von dakota, über das Menü **<Zertifikate> <Sicherung importieren >**. Der Assistent erwartet über den folgenden Dialog die Angabe des Speicherortes Ihres Sicherungsverzeichnisses:

Geben Sie den Speicherort der Sicherung an und wählen Sie Öffnen. Sie haben nachfolgend noch die Möglichkeit einen neuen Zertifikatsnamen zu vergeben.



Anschließend importiert dakota die Sicherung und meldet den Erfolg am Bildschirm.

Hinweis: Sie haben auch die Möglichkeit durch einen Doppelklick direkt auf die gewünschte Datei im dakota_S- bzw. im dakota_LE-Ordner das Zertifikat einzulesen.

An dem Dateinamen einer Sicherung, welche mit dakota 7.0 erstellt wurde, kann erkannt werden, in welchem Status sich das Zertifikat befindet.

- **A**ntrag gestellt
  dakotaag/le_**A**_<ID>_<yyyyMMdd_HHmmss>.dag/dle
  Diese Sicherung beinhaltet den Status, dass ein Zertifikatsantrag an das ITSG-Trust Center übermittelt wurde.

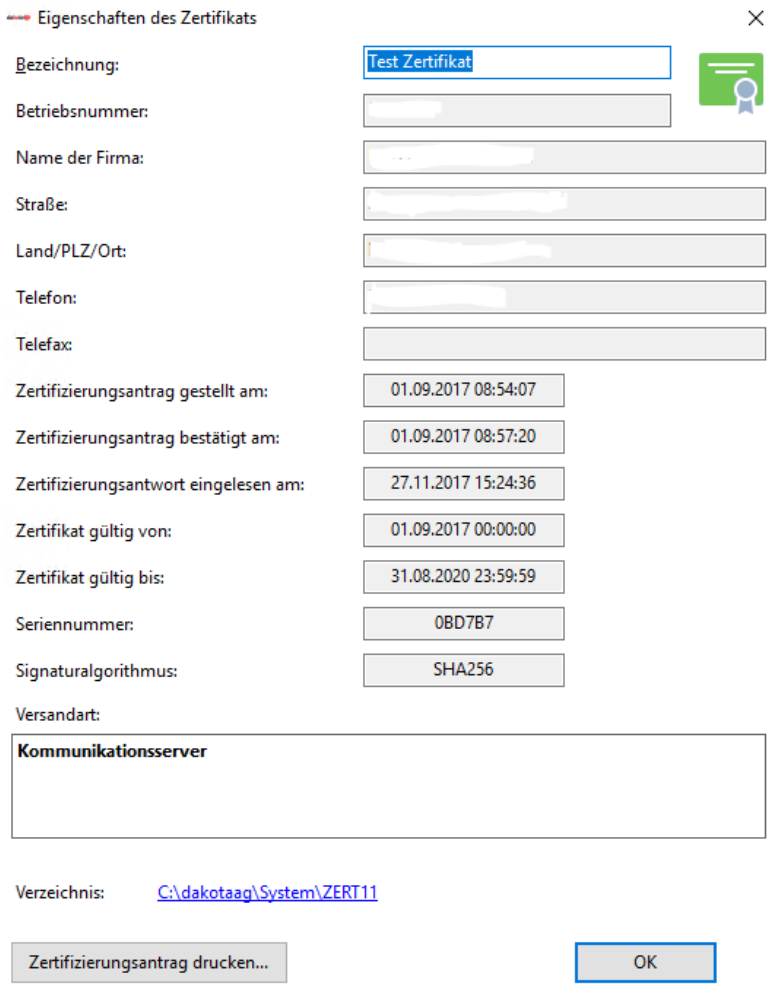
- Antrag **b**estätigt
  dakotaag/le _**B**_<ID>_<yyyyMMdd_HHmmss>.dag/dle
  In dieser Sicherung wurde der Zertifikatsantrag, welcher an das ITSG-Trust Center übermittelt wurde, beim ITSG-Trust Center bestätigt und somit die Erstellung beauftragt.

- Zertifikatsantwort **v**erarbeitet
  dakotaag/le _**N**_<ID>_<yyyyMMdd_HHmmss>.dag/dle
  Diese Sicherung enthält das vollständige Zertifikat, mit der Zertifikatsantwort vom ITSG-Trust Center.

6.10 Eigene Schlüsseldaten

Die Informationen bezüglich Ihres eigenen Schlüssels können Sie jederzeit in der dakota-Software einsehen. Sie finden Ihre Eingaben über die Funktion **<Zertifikate>**.

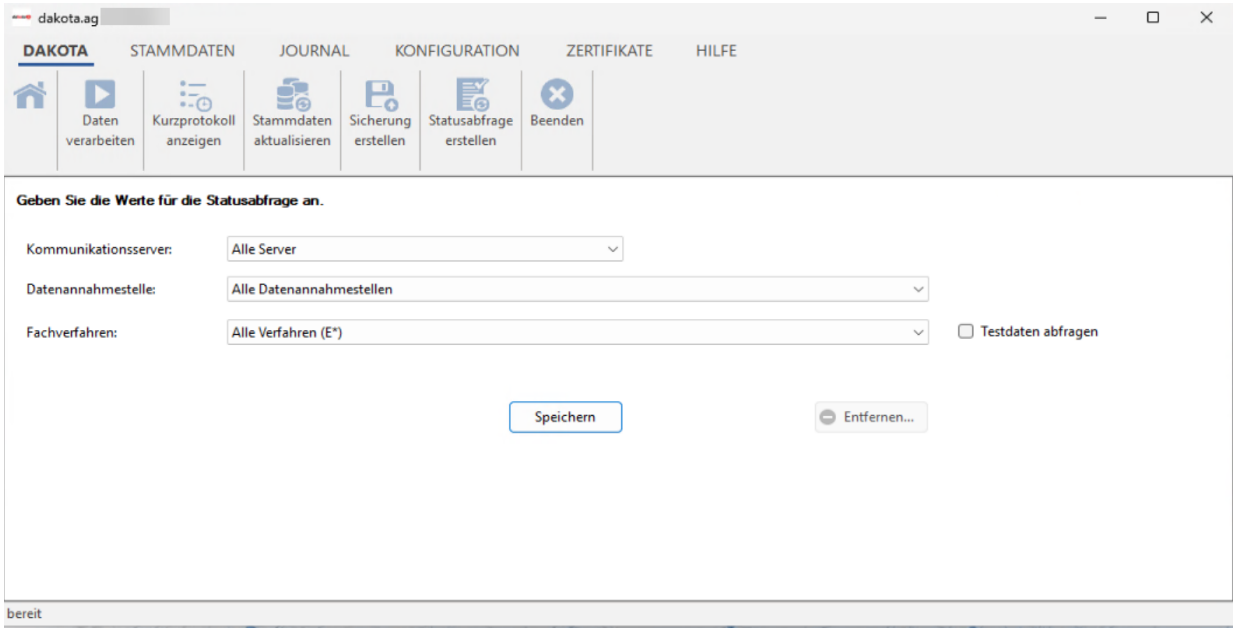
Wählen Sie hierfür auf der Hauptmaske von dakota das Menü **<Zertifikate>** und anschließend die Funktion **<Eigenschaften>.**



6.11 Statusabfrage

Die Funktion **<Statusabfrage erstellen>** erreichen Sie nur über die Hauptmaske von dakota (diese Funktion gibt es in dakota.le nicht) über das Menü **<dakota>** (nicht in allen Versionen von dakota.ag vorhanden).

Mit der Hilfe dieser Funktion können Statusabfragen für den Kommunikationsserver individuell erstellt werden.

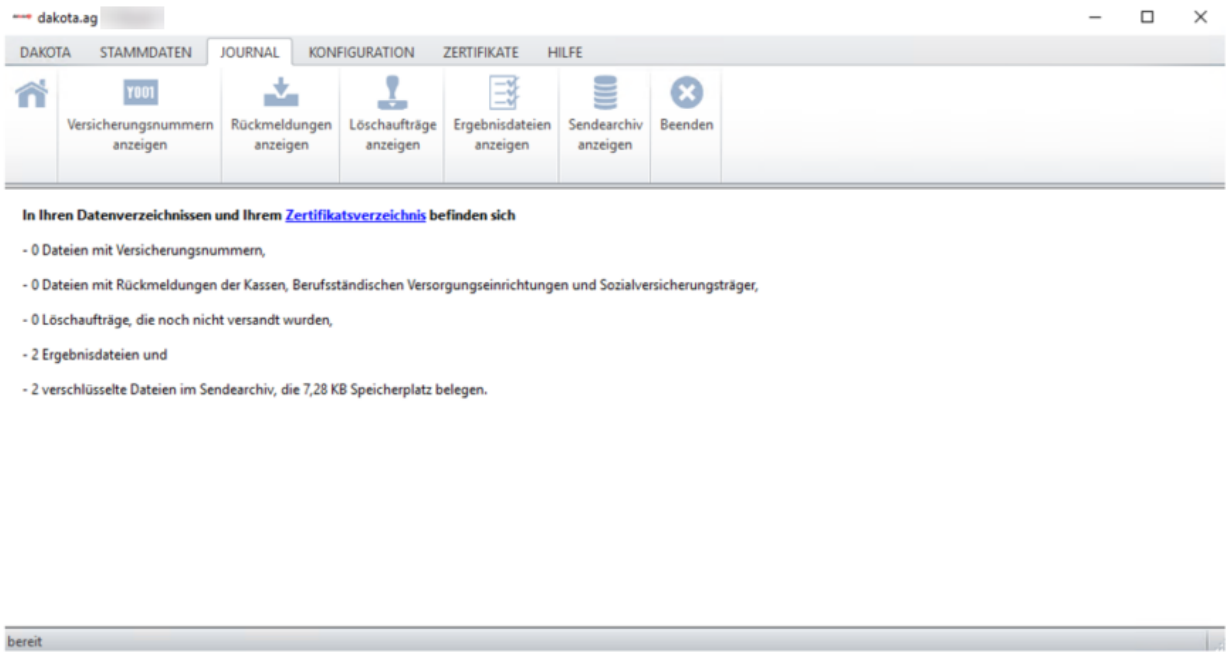


6.12 Journal

Die Funktion **<Journal>** (diese Funktion gibt es in dakota.le nicht) erreichen Sie über die Hauptmaske von dakota (nicht in allen Versionen von dakota.ag vorhanden).

Das Journal dient dazu, Dateien im dakota-Verzeichnis zu verwalten und ggf. zu bereinigen. Die Funktion scannt alle Verzeichnisse von dakota.ag auf Rückmeldungen, Löschdateien, Ergebnisdateien und das Sendearchiv.

Sollten Dateien in den gescannten Verzeichnissen vorhanden sein, so können diese mit dem Tool gesichtet werden. Die Dateien können je nach Art der Dateien angezeigt, archiviert, verarbeitet oder gelöscht werden.



7 Häufig gestellte Fragen

7.1 Allgemeine Fragen zu dakota.ag

- **Wo kann ich Informationen über den elektronischen Datenaustausch mit den Sozialversicherungsträgern erhalten?**
  Die rechtlichen und technischen Vorgaben für die Übermittlung elektronischer Daten an die Sozialversicherungsträger finden Sie im Internet unter www.gkv datenaustausch.de.

- **Wo kann ich dakota.ag beziehen?**
  Die ITSG GmbH ist der Hersteller von dakota.ag, vertreibt jedoch dakota.ag ausschließlich an Wiederverkäufer. Möchten Sie als Arbeitgeber dakota.ag einsetzen, wenden Sie sich bitte an das Softwarehaus Ihres Entgeltabrechnungssystems.

- **Wo erhalte ich Unterstützung für mein dakota.ag-Problem?**
  Unterstützung erhalten Sie ausschließlich von Ihrem Softwarehaus. Bitte wenden Sie sich mit Ihren Anfragen an Ihren Softwarepartner.

- **Wozu gibt es eigentlich ein Trust Center?**
  Ein Trust Center erstellt digitale Zertifikate (Schlüssel) für den gesicherten Datenaustausch im Gesundheitswesen und stellt die öffentlichen Schlüssel bereit. Weitere Infos erhalten Sie unter der Kurzdarstellung des Trust Centers auf www.trustcenter.info.

- **Was ist ein Zertifikat?**
  Das Zertifikat wird für die Verschlüsselung benötigt. Vereinfacht ausgedrückt ist es der von einem Trust Center bestätigte öffentliche Schlüssel eines jeden Teilnehmers im Datenaustauschverfahren. Das Zertifikat hat eine begrenzte Gültigkeitsdauer von drei Jahren und kann nach Ablauf nicht weiterverwendet werden.

- **Wann muss ich ein neues Zertifikat beim Trust Center beantragen?**
  Das Zertifikat hat eine begrenzte Laufzeit von drei Jahren. dakota.ag warnt Sie vor dem Ablauf dieses Zeitraumes (z. B. 10 Tage vor Ablauf). Nach diesem Ablauf-Hinweis bearbeiten Sie Ihre Monatsmeldungen noch wie gewohnt und beantragen danach einen neuen Schlüssel; der dakota.ag -Assistent führt Sie durch die einzelnen Schritte.

- **Wann ändern sich die elektronischen Schlüssel der Annahmestellen?**
  Die Annahmestellen der Sozialversicherungsträger erstellen alle drei Jahre einen neuen Schlüssel. Der nächste Schlüsselwechsel findet am 31.12.2027 statt. Dadurch ist eine Aktualisierung der öffentlichen Schlüsseldatei (annahme-pkcs.agv) nur zum Jahresanfang der Drei-Jahres-Frist notwendig.

- **Ich bin Arbeitgeber mit mehreren Betriebsnummern, welche muss ich angeben?**
  Bei der Abrechnung von mehreren Betriebsnummern erstellen Sie nur für die Betriebsnummer des Abrechnungsbetriebes (für diesen Betrieb ist auch die Zulassung zur DEÜV erfolgt) einen Schlüssel und versenden damit die kompletten Daten.

- **Wie finde ich die Betriebsnummern der Sozialversicherungsträger?**
  Informationen über alle Betriebsnummern der Sozialversicherungsträger finden Sie unter www.gkv-datenaustausch.de. Dort können Sie auch eine Beitragssatzdatei mit den Informationen zu der Betriebsnummer der Sozialversicherungsträger herunterladen.

7.2 Allgemeine Fragen zu dakota.le

- **Wo kann ich Informationen über den elektronischen Datenaustausch mit Sozialversicherungsträgern erhalten?**
  Die rechtlichen und technischen Vorgaben für die Übermittlung elektronischer Daten an die Sozialversicherungsträger finden Sie unter www.gkv-datenaustausch.de.

- **Wo kann ich dakota.le beziehen?**
  Die ITSG GmbH ist der Hersteller von dakota.le, vertreibt jedoch dakota.le ausschließlich an Wiederverkäufer. Möchten Sie als Leistungserbringer dakota.le einsetzen, wenden Sie sich bitte an das Softwarehaus Ihres Abrechnungssystems.

- **Wo erhalte ich Unterstützung für mein dakota.le-Problem?**
  Unterstützung erhalten Sie ausschließlich von Ihrem Softwarehaus. Bitte wenden Sie sich mit Ihren Anfragen an Ihren Softwarepartner.

- **Wozu gibt es eigentlich ein Trust Center?**
  Ein Trust Center erstellt digitale Zertifikate (Schlüssel) für den gesicherten Datenaustausch im Gesundheitswesen und stellt die öffentlichen Schlüssel bereit. Weitere Infos erhalten Sie unter der Kurzdarstellung des Trust Centers auf www.trustcenter.info.

- **Was ist ein Zertifikat?**
  Das Zertifikat wird für die Verschlüsselung benötigt. Vereinfacht ausgedrückt ist es der von einem Trust Center bestätigte öffentliche Schlüssel eines jeden Teilnehmers im Datenaustauschverfahren. Das Zertifikat hat eine begrenzte Gültigkeitsdauer und kann nach Ablauf nicht weiterverwendet werden.

- **Wann muss ich ein neues Zertifikat beim Trust Center beantragen?**
  Das Zertifikat hat eine begrenzte Laufzeit von einem Jahr. dakota.le warnt Sie vor dem Ablauf dieses Zeitraumes (z. B. 10 Tage vor Ablauf). Nach diesem Ablauf-Hinweis bearbeiten Sie Ihre Dateien noch wie gewohnt und beantragen danach einen neuen Schlüssel; der dakota.le -Assistent führt Sie durch die einzelnen Schritte.

- **Wann ändern sich die elektronischen Schlüssel der Annahmestellen?**
  Die Annahmestellen der Sozialversicherungsträger erstellen alle drei Jahre einen neuen Schlüssel. Der nächste Schlüsselwechsel findet am 31.12.2027 statt. Dadurch ist eine Aktualisierung der öffentlichen Schlüsseldatei (annahme-pkcs.key) nur zum Jahresanfang der Drei-Jahres-Frist notwendig.

- **Wie erhalte ich die Zulassung zum maschinellen Abrechnungsverfahren?**
  Voraussetzung für eine Teilnahme ist, dass Sie über ein Institutionskennzeichen (IK-Nummer) verfügen und sich bei einer Kassenart zum maschinellen Abrechnungsverfahren anmelden. Nähere Infos hierzu finden Sie unter: www.gkv-datenaustausch.de.

7.3 Technisch orientierte Fragen

- **Kann ich dakota auch unter Linux (oder andere) einsetzen?**
  Nein, dakota unterstützt ausschließlich Windows Betriebssysteme. Die technischen Daten finden Sie in der Produktinformation von dakota.

- **Welche Internet-Provider unterstützt dakota?**
  Ihr Provider muss Ihnen die Adressen für die E-Mail-Dienste (SMTP und POP) mitteilen, damit diese Einstellungen in dakota E-Mail eingetragen werden können. Üblicherweise werden diese Adressen von allen Internet-Providern geliefert.

- **Welche Systemrechte benötige ich bei Windows?**
  Für die Installation sind Administrator-Rechte notwendig. Sehen Sie dazu im Handbuch nach und sprechen Sie ggf. mit Ihrem Softwarehaus.

- **Wie stelle ich die E-Mail-Adressen der Annahmestellen ein?**
  Die E-Mail-Adressen der Annahmestellen sind in dakota hinterlegt. Zur Aktualisierung nutzen Sie bitte unter **<Stammdaten> <über das Internet herunterladen>.**

- **Wie verarbeite ich die E-Mail vom Trust Center mit meinem Zertifikat?**
  Vom ITSG-Trust Center erhalten Sie eine E-Mail mit drei Anhängen, Ihr Zertifikat (anwender.p7c), die öffentliche Schlüsselliste und diese beiden Dateien noch einmal in Form einer ZIP-Datei. Zusätzlich ist in dieser E-Mail ein „Link“ vorhanden, der Sie ebenfalls zu Ihrem Zertifikat führt. Speichern Sie die beiden Dateien in das Datenverzeichnis von dakota (z. B. c:\dakotaag). Zum Speichern eines Dateianhanges klicken Sie die Datei mit der rechten Maustaste an.

  Nach dem Speichern verarbeiten Sie die Dateien im dakota-Assistenten.

- **Wie verarbeite ich das Schlüsselverzeichnis der Annahmestellen?**
  Vom ITSG-Trust Center erhalten Sie eine E-Mail mit einem Anhang oder Sie kopieren die Datei von der ITSG Homepage http://www.trustcenter.info. Speichern Sie die Datei in das Datenverzeichnis von dakota (z. B. c:\dakotaag).

  Nach dem Speichern verarbeiten Sie die Datei im dakota-Assistenten.

- **Wie kann ich dakota nach einem Systemcrash wiederherstellen?**
  Informieren Sie Ihren Softwarepartner. Unter dessen Anweisung könnte die vorhandene Datensicherung Ihres Systems zurückgespielt werden.

  dakota sichert die Schlüsseldaten nach der Inbetriebnahme in einem separaten Verzeichnis. Diese Daten können zur Rekonstruktion des verloren gegangenen Schlüssels unter Anleitung Ihres Softwarehauses genutzt werden.