



Benutzer Handbuch

Version 4.1

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 irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, ob die Vervielfältigung oder Übertragung auf elektronischem, photo-optischem oder mechanischem Wege geschieht.

© ITSG GmbH 2008

Microsoft, MS, Windows 2000, Windows XP, Windows Vista, MS Office, MS Access sind eingetragene Marken der Microsoft Corporation.

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

ITSG GmbH
Daimlerstraße 11
63110 Rodgau

Inhaltsverzeichnis

| | | |
|---------|---|----|
| 1 | Einleitung | 4 |
| 1.1 | dakota | 4 |
| 1.2 | Das Sicherheitsverfahren im Gesundheitswesen | 5 |
| 2 | Inbetriebnahme | 6 |
| 2.1 | Kurzbeschreibung | 6 |
| 2.2 | Installation | 7 |
| 2.3 | Inbetriebnahme mit dem dakota-Assistenten..... | 10 |
| 2.3.1 | Programmstart | 10 |
| 2.3.2 | Konfiguration der Versandart..... | 10 |
| 2.3.2.1 | Versandart dakota E-Mail (SMTP) | 11 |
| 2.3.2.2 | Versandart E-Mail-Standardprogramm..... | 13 |
| 2.3.2.3 | Versandart Verzeichnisausgabe | 15 |
| 2.3.3 | Konfiguration des Schlüssels (Zertifizierungsantrag) | 16 |
| 2.3.3.1 | Erfassen der Adressdaten..... | 17 |
| 2.3.3.2 | Erfassen des verantwortlichen Ansprechpartners | 18 |
| 2.3.3.3 | Erfassen des Schlüssel-Passwortes | 18 |
| 2.3.3.4 | Zusammenfassung der Angaben | 19 |
| 2.3.3.5 | Fertigstellen und Aussendung des Schlüssels an das Trust Center | 20 |
| 2.3.3.6 | Einlesen des Schlüssels vom Trust Center | 22 |
| 3 | Verarbeitung..... | 27 |
| 3.1 | Kurzbeschreibung | 27 |
| 3.2 | Programmstart | 28 |
| 3.3 | Daten verarbeiten mit Direktaufruf von dakota | 29 |
| 3.3.1 | Daten verarbeiten..... | 29 |
| 3.3.2 | Versenden mit E-Mail: dakota E-Mail | 30 |
| 3.3.3 | Versenden mit dem Standard-E-Mail Programm: Outlook Express | 30 |
| 3.3.4 | Versenden mit Verzeichnis Ausgabe..... | 30 |
| 3.4 | Verschlüsseln und Versenden integriert in die Fachanwendung..... | 31 |
| 4 | Protokollierung | 32 |
| 4.1 | Kurzbeschreibung | 32 |
| 4.2 | Langprotokoll..... | 33 |
| 4.3 | Kurzprotokoll | 34 |
| 4.3.1 | Detailansicht | 34 |
| 5 | dakota-Aktualisierung..... | 36 |
| 5.1 | Kurzbeschreibung | 36 |
| 5.2 | Neuer Schlüssel | 37 |
| 6 | Optionen | 38 |
| 6.1 | Allgemeine Optionen | 39 |
| 6.2 | Optionen für die Verschlüsselung..... | 40 |
| 6.3 | Optionen für die Entschlüsselung..... | 41 |
| 6.4 | Optionen für das Stammdatenupdate..... | 42 |
| 6.5 | Sicherung erstellen | 43 |
| 6.6 | Sicherung importieren | 44 |
| 6.7 | Eigene Schlüsseldaten..... | 45 |
| 6.8 | Erweiterte SMTP Optionen..... | 46 |
| 6.9 | Zertifikatsverwaltung | 47 |
| 7 | Häufig gestellte Fragen | 49 |
| 7.1 | Allgemeine Fragen zu dakota ^{ag} | 49 |
| 7.2 | Allgemeine Fragen zu dakota ^{le} | 51 |
| 7.3 | Technisch orientierte Fragen..... | 52 |
| 8 | Änderungshistorie | 57 |
| 9 | Index | 58 |

1 Einleitung

1.1 dakota

dakota ist ein Programm zur Unterstützung der gesicherten Internet-Kommunikation zwischen Arbeitgebern bzw. "sonstigen Leistungserbringern" und den gesetzlichen Krankenkassen. 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 gesetzlichen Krankenkassen erfüllt. Alle Nutzdaten werden vor dem Versand verschlüsselt.

Der Name dakota bezeichnet eine Produktfamilie der ITSG GmbH und steht als Synonym für '**D**atenaustausch und **K**ommunikationen 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 sichergestellt werden wie beim herkömmlichen papiergebundenen Abrechnungsverfahren, z. B. durch verschlossene Umschläge und persönliche Unterschriften. Verschlüsselung und digitale Signatur auf der Grundlage kryptographischer Verfahren sind hierfür geeignete Maßnahmen.

Jeder Teilnehmer am Datenaustausch 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 öffentlicher als auch privater 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 digitaler Signatur. Der Absender signiert Daten mit seinem privaten Schlüssel, so dass jeder mit dem allgemein bekannten öffentlichen Schlüssel des Absenders die digitale Signatur prüfen kann. Aus diesem Grunde 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 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. Sie können die Installation mit einem Assistenten ausführen oder Ihr Softwarehaus integriert die dakota-Software in die Fachanwendung.
- **Die Konfiguration**
dakota bietet Ihnen einen Software-Assistenten um die Versandart einzustellen und um Ihren Schlüssel beim Trust Center zu beantragen.
- **Konfiguration Ihrer Versandart**
Es ist möglich die Daten für die Krankenkassen an Ihr Standard-E-Mail-Programm zu übergeben oder Sie versenden die Daten mit dakota-E-Mail. Dakota-E-Mail bietet Ihnen die Möglichkeit die Daten direkt (per SMTP Protokoll) in das Internet zu versenden. Beim ersten Start von dakota führt Sie der Assistent automatisch durch die Einrichtung und unterstützt Sie bei der Eingabe der notwendigen Angaben.
- **Konfiguration Ihres Schlüssels**
Für den verschlüsselten Datenaustausch mit den gesetzlichen Krankassen ist es notwendig einen Antrag auf Zertifizierung Ihres Schlüssels bei einem Trust Center zu stellen. Dieser Antrag besteht aus den folgenden Bestandteilen:
 - **die crq- bzw. p10-Datei**, wird von dakota automatisch per E-Mail an das Trust Center gesendet,
 - **den ausgefüllten Zertifizierungsantrag** (2 Seiten) und
 - **eine Kopie vom Personalausweis** des verantwortlichen Ansprechpartners.

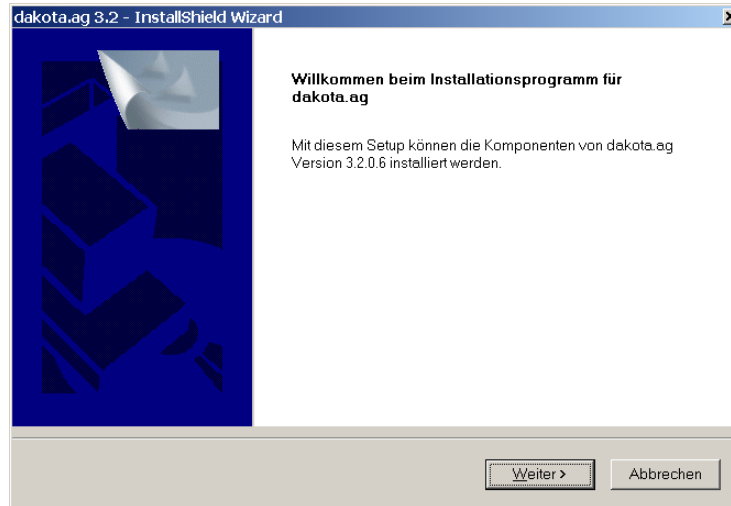
Wenn Sie einen Schlüssel als sonstiger Leistungserbringer (Physiotherapie, Ergotherapie, etc.) beantragen möchten, benötigen Sie noch zusätzlich eine

- **Kopie des IK-Nummern Vergabebescheides.**
Diesen Vergabebescheid erhalten Sie von der Arbeitsgemeinschaft Institutions-Kennzeichen in Sankt Augustin.
- **Einlesen der Antwort vom Trust Center**
Das Trust Center zertifiziert Ihren Schlüssel für die Teilnahme am Datenaustausch im Deutschen Gesundheitswesen. Zusätzlich erhalten Sie vom Trust Center alle notwendigen Schlüssel der Datenannahmestellen.
- **Versenden der Daten an die Krankenkassen und andere Empfänger**
Alle Dateien werden vor dem Versenden sicher verschlüsselt und automatisch per E-Mail versendet. 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**.

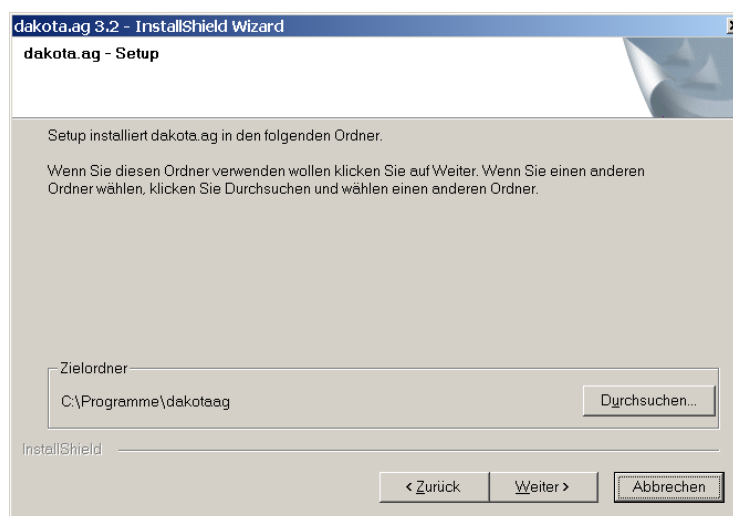
Der Installations-Assistent begrüßt Sie und erläutert Ihnen, welche dakota-Variante und welche Version Sie installieren können.




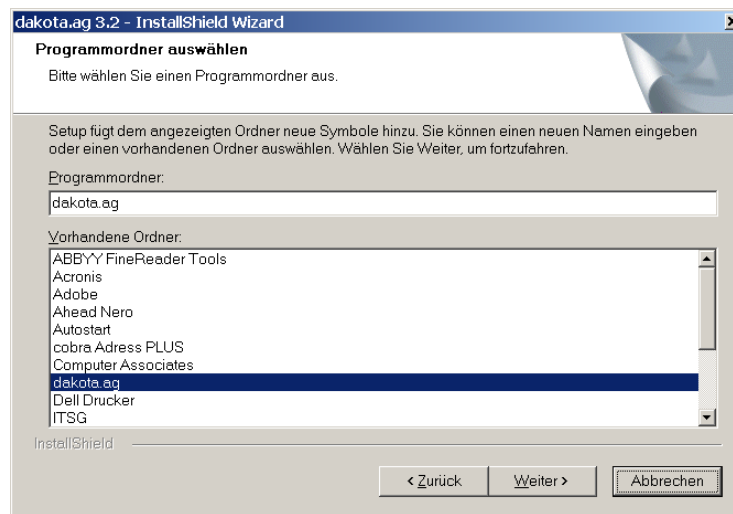
Hinweis: Es ist möglich die Installation ohne einen Dialog mit dem Benutzer durchzuführen. D. h. es kann sein, dass dakota bereits automatisch auf Ihrem Computer installiert wurde.



Wenn Sie die Installation beenden möchten können Sie hierfür **Abbrechen** nutzen.

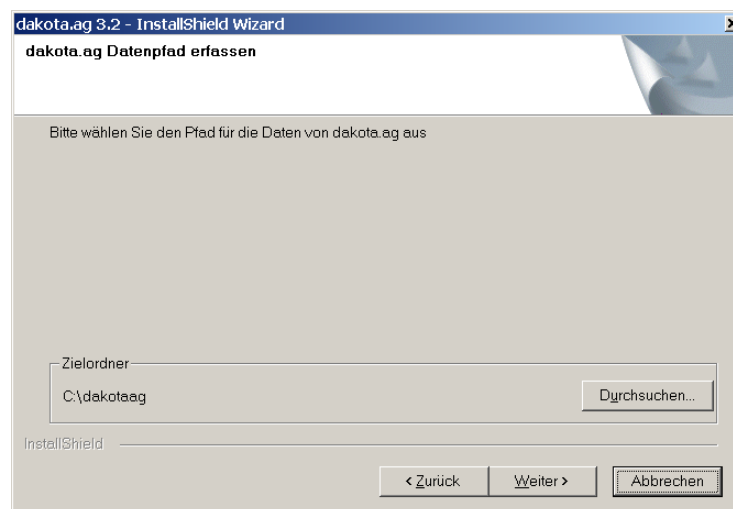
Der Installations-Assistent wird nun den Programm-Pfad von dakota standardmäßig in das Verzeichnis **C:\Programme\dakotaag** installieren. Wenn Sie den Programm-Pfad wechseln möchten, wählen Sie bitte **Durchsuchen...** und ändern Sie die Pfadangabe auf das gewünschte Verzeichnis. Sobald Sie den gewünschten Programm-Pfad angegeben haben, wählen Sie bitte **Weiter >** um mit der Installation fortzufahren.



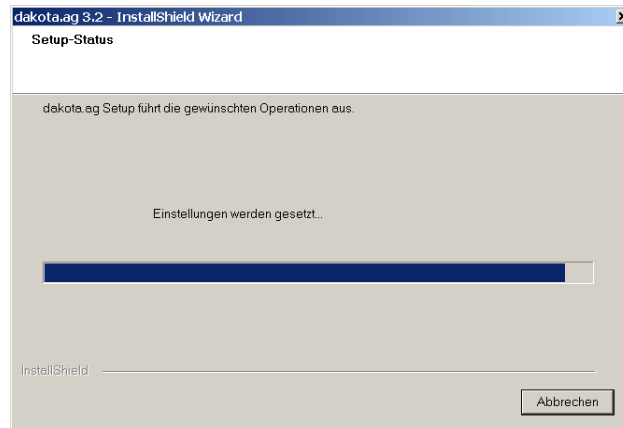
Auf der folgenden Maske können Sie eine gewünschte Verknüpfung unter **Start/Programme** in Ihrem Windows Betriebssystem anlegen. Wählen Sie  um mit der Installation fortzufahren.



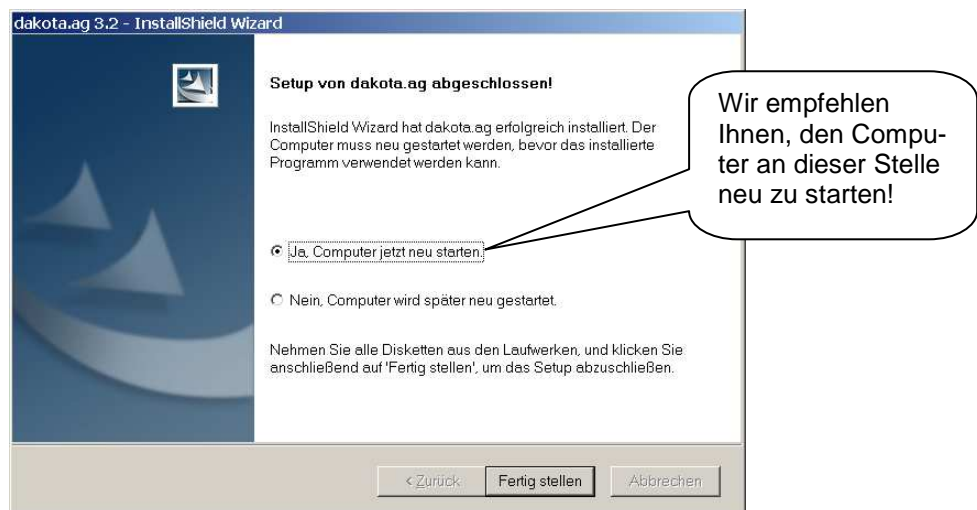
Im folgenden Schritt müssen Sie einen Datenpfad für dakota angeben. In diesem Verzeichnis werden Ihre Benutzerdaten abgelegt, wie z. B. Ihre Verarbeitungsprotokolle. Wenn Sie den Datenpfad wechseln möchten, wählen Sie bitte  und ändern Sie die Pfadangabe auf das gewünschte Verzeichnis. Sobald Sie den gewünschten Datenpfad angegeben haben, wählen Sie bitte , um mit der Installation fortzufahren.



Die Software wird nun auf Ihrem Computer installiert. Bitte haben Sie ein wenig Geduld. Die Installation ist erst abgeschlossen, wenn der Fortschrittsbalken die **100%** erreicht hat.



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


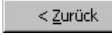
2.3.1 Programmstart

Der dakota-Assistent wird in der Regel von Ihrem Softwarehaus in Ihre Fachanwendung eingebunden. Weitere Informationen zu diesem *Execute-Modus* finden Sie im technischen Handbuch zu dakota. Oder möchten Sie die dakota-Inbetriebnahme durch den Assistenten direkt starten?

⇒ Wählen Sie hierfür *'Start → Programme → Dakota → dakota...'*.

Beim erstmaligen Aufruf nach der Installation wird der Assistent von dakota automatisch gestartet. Für einen wiederholten Aufruf des Assistenten

⇒ Wählen Sie aus dem dakota-Hauptmenü *'Extras → Assistent'*.

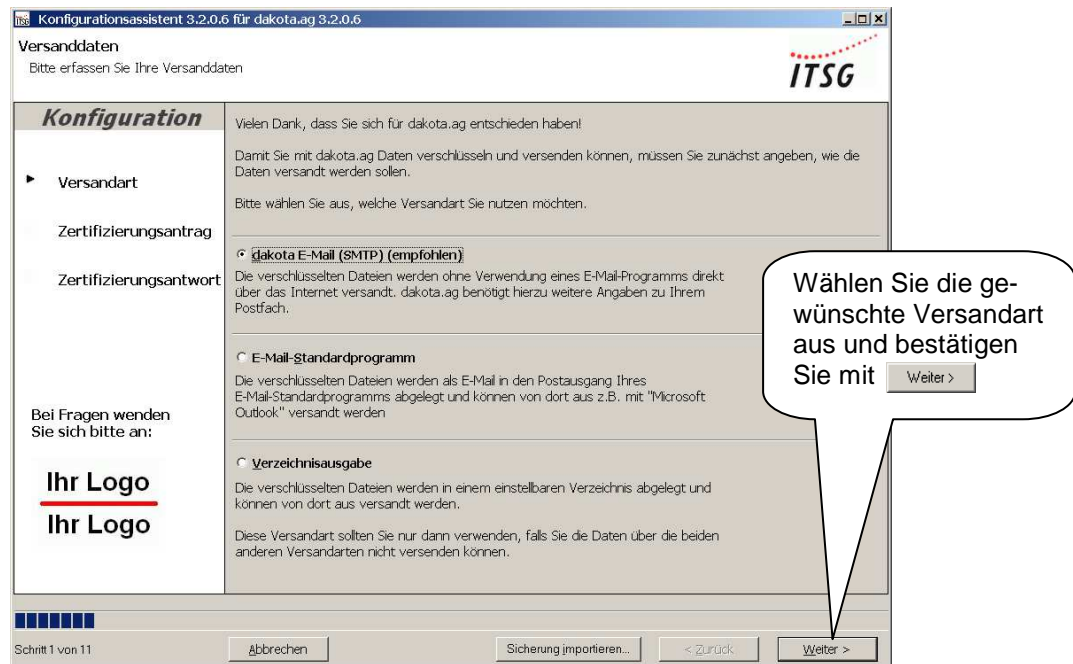
Der Assistent führt Sie schrittweise über  durch alle erforderlichen Punkte für die Inbetriebnahme von dakota. Die einzelnen Schritte sind in den folgenden Unterkapiteln beschrieben. Falls Sie einen Schritt im Assistenten wiederholen möchten, dann wählen Sie einfach die Funktion  und korrigieren Sie Ihre Eingaben.

2.3.2 Konfiguration der Versandart

Damit Sie die verschlüsselten Dateien per E-Mail an die Datenannahmestellen der gesetzlichen Krankenversicherung senden können, müssen Sie in dakota einstellen, welche Versandart Sie verwenden möchten.

Die folgenden Versandarten stehen Ihnen 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) in das Internet versenden. Wenn Sie diese Versandart einstellen möchten, lesen Sie bitte im Kapitel 2.3.2.1 Versandart dakota E-Mail (SMTP).
- **E-Mail-Standardprogramm**
Die Versandart übergibt die verschlüsselten Dateien komfortabel an Ihr bereits genutztes E-Mail-Programm. Wenn Sie diese Versandart einstellen möchten, lesen Sie bitte im Kapitel 2.3.2.2 weiter.
- **Verzeichnisausgabe**
Falls Ihnen keine der vorgenannten Versandarten entspricht, bieten wir Ihnen die Möglichkeit die verschlüsselten Dateien in ein Ausgabeverzeichnis zu übergeben. Wenn Sie diese Versandart einstellen möchten, lesen Sie bitte im Kapitel 2.3.2.3 weiter.



Hinweis: Wenn Sie bereits eine Sicherung von dakota haben, können Sie diese Sicherung über die Funktion

Sicherung importieren...

2.3.2.1 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.

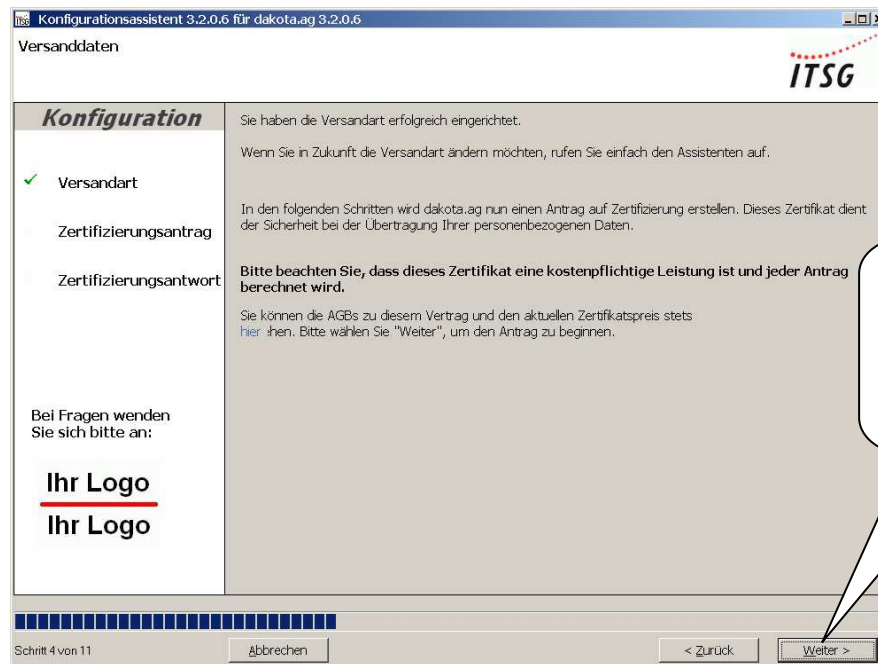
Hinweis: Sie finden in der Auswahlmöglichkeit **Provider** eine Liste der meistgenutzten E-Mail-Provider.

- **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 Passwort durchzuführen. Wenn der von Ihnen genutzte SMTP-Server diese Anmeldung verlangt, wählen Sie diese Option an und geben Sie Ihren Benutzernamen und Ihr Passwort für dieses E-Mail-Konto ein. Bei dieser Option fragen Sie ggf. bei Ihrem Systemadministrator oder dem Anbieter Ihres E-Mail-Kontos nach.

Welche erweiterten Optionen Sie noch einstellen können, finden Sie im Kapitel 6.8 Erweiterte SMTP Optionen

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

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



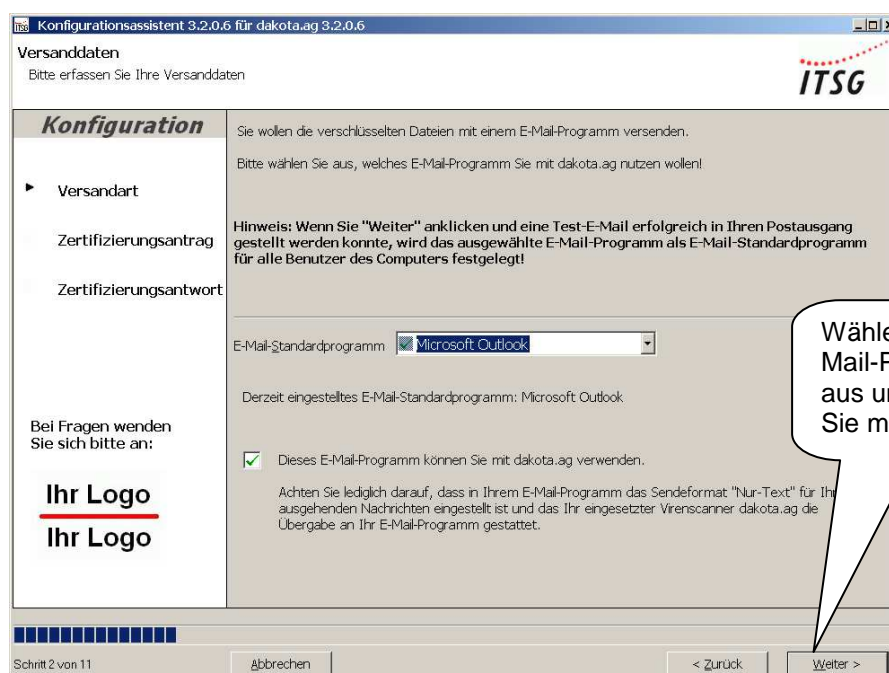
Sie haben erfolgreich die Versandart eingerichtet. In den folgenden Schritten erzeugen Sie Ihren Schlüssel und stellen einen Antrag beim Trust Center. Bitte lesen Sie nun im Kapitel 2.3.3 Konfiguration des Schlüssels (Zertifizierungsantrag) weiter, um die Konfiguration Ihres Schlüssels durchzuführen.

2.3.2.2 Versandart E-Mail-Standardprogramm

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

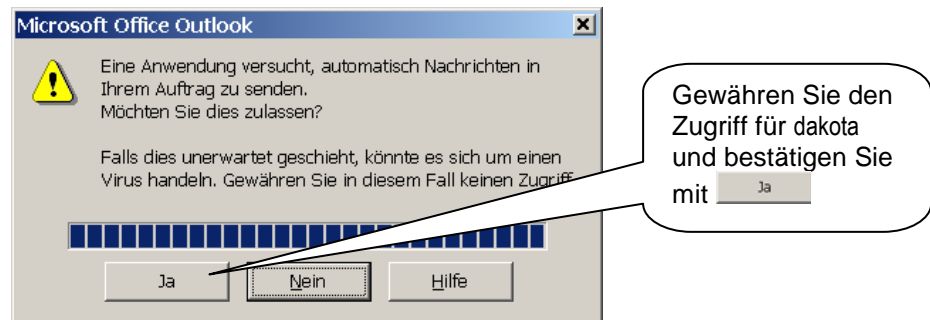
Über die Auswahlbox können Sie das Standard-E-Mail-Programm Ihres Systems einstellen.

Hinweis: Bitte beachten Sie, dass die Umstellung des Standard-E-Mail-Programmes auch für andere Software-Produkte auf Ihrem Computer vorgenommen wird.



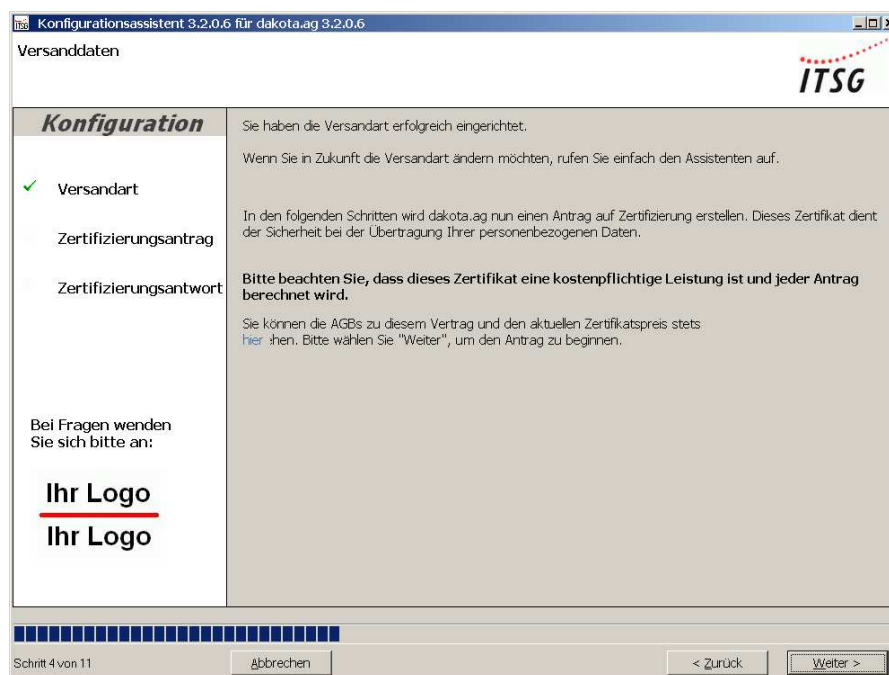
Im Anschluss versucht dakota Ihre Versandart zu testen. Hierbei versendet dakota eine E-Mail zum Test an die E-Mail-Adresse info-pas@itsg.de.

Viele E-Mail-Programme und Betriebssysteme verfügen über Sicherheitsmechanismen um Ihren Computer gegen die Verbreitung von Viren zu schützen. Es kann sein, dass Sie die folgende Meldung am Bildschirm erhalten:



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: Sie müssen die Test-E-Mail nicht an die Adresse info-pas@itsg.de senden. Bei dieser Test-E-Mail werden keine persönlichen Daten oder Registrierungsinformationen in das Internet gesendet. Der Test dient lediglich um technisch sicherzustellen, dass der Versand über Ihr E-Mail-Konto funktioniert.



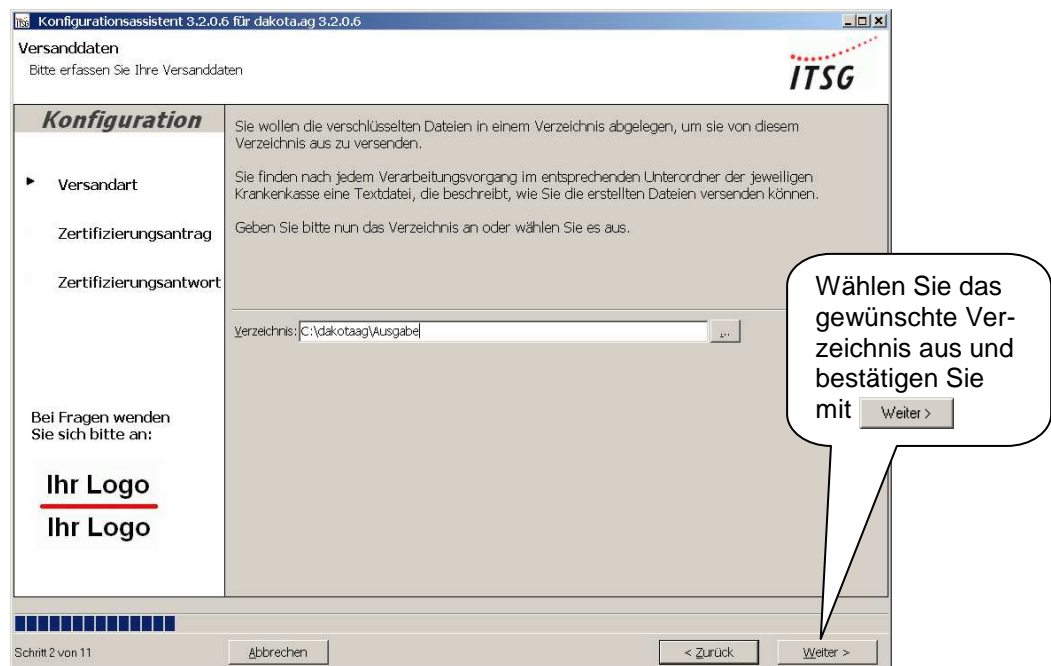
Sie haben erfolgreich die Versandart eingerichtet. In den folgenden Schritten erzeugen Sie Ihren Schlüssel und stellen einen Antrag beim Trust Center. Bitte lesen Sie nun im Kapitel 2.3.3 Konfiguration des Schlüssels (Zertifizierungsantrag) weiter, um die Konfiguration Ihres Schlüssels durchzuführen.

2.3.2.3 Versandart Verzeichnisausgabe

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

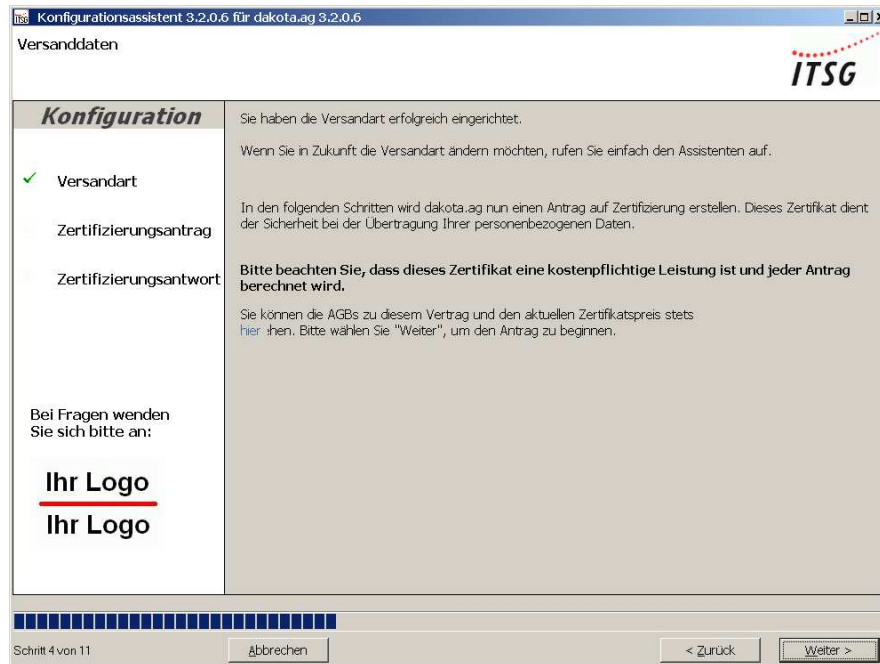
- **Verzeichnis:** Geben ein Datei-Verzeichnis an, in welches dakota die verschlüsselten Nachrichten ablegt.

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



Im Anschluss überprüft dakota ob es möglich ist in das Ausgabeverzeichnis Dateien abzulegen.





Sie haben erfolgreich die Versandart eingerichtet. In den folgenden Schritten erzeugen Sie Ihren Schlüssel und stellen einen Antrag beim Trust Center. Bitte lesen Sie nun im Kapitel 2.3.3 Konfiguration des Schlüssels (Zertifizierungsantrag) weiter, um die Konfiguration Ihres Schlüssels durchzuführen.

2.3.3 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,**
...dann 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,**
...dann geben Sie bitte auf der Maske Ihr **Institutionskennzeichen (IK)** ein. Ein Institutionskennzeichen erhalten Sie von der SVI Arbeitsgemeinschaft Institutionskennzeichen, Postfach 2052, 53743 Sankt Augustin.

2.3.3.1 Erfassen der Adressdaten

Im folgenden Schritt werden Sie nach Ihren Adressangaben gefragt. Alle Angaben, die mit einem * gekennzeichnet sind, müssen Sie ausfüllen.

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

2.3.3.2 Erfassen des verantwortlichen Ansprechpartners

Im folgenden Schritt müssen Sie einen verantwortlichen Ansprechpartner für den Schlüssel benennen. Dieser verantwortliche Ansprechpartner muss eine natürliche Person sein und nicht etwa eine Abteilung in Ihrem Unternehmen.

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

Konfigurationsassistent 3.2.0.6 für dakota.ag 3.2.0.6

Zertifizierungsantrag
Bitte erfassen Sie Ihre Daten für den Zertifizierungsantrag

Konfiguration

- ✓ Versandart
- Zertifizierungsantrag
- Zertifizierungsantwort

Bei Fragen wenden Sie sich bitte an:

Ihr Logo
Ihr Logo

Geben Sie bitte einen verantwortlichen Ansprechpartner für das Zertifikat an. Bitte beachten Sie, dass der angegebene Ansprechpartner eine Kopie seines Personalausweises (Führerschein oder Reisepass sind auch möglich) befügen muss.

Bitte achten Sie darauf, keine Sonderzeichen und Umlaute (z. B.: +, /, *, etc.) zu verwenden.

Ansprechpartner: Manfred Mustermann

Erfassen Sie einen Ansprechpartner und bestätigen Sie mit **Weiter >**

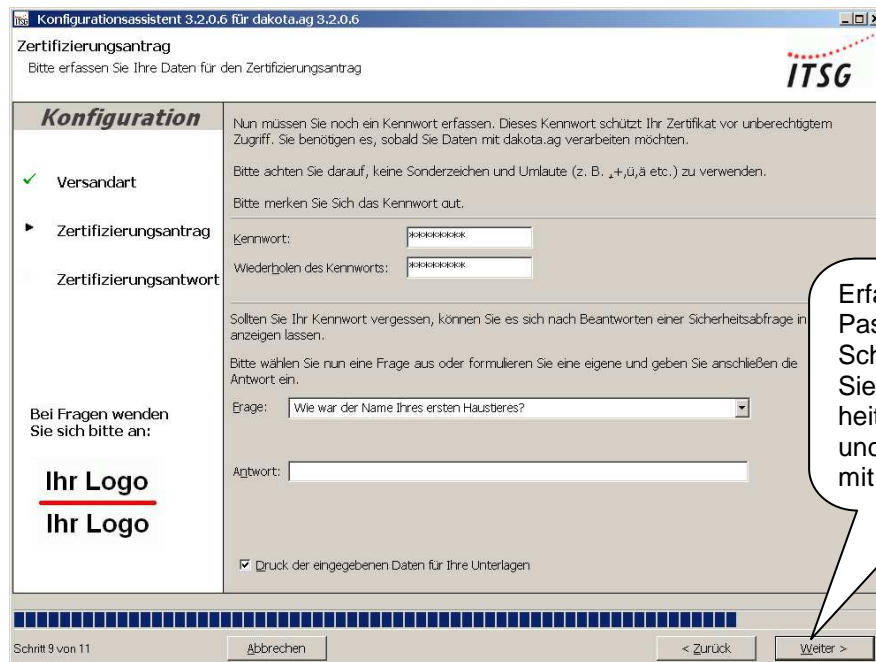
Schritt 8 von 11

Abbrechen < Zurück Weiter >

2.3.3.3 Erfassen des Schlüssel-Passwortes

Damit Ihr Schlüssel vor unberechtigtem Zugriff geschützt wird, müssen Sie ein Passwort vergeben. **Bitte merken Sie sich das Passwort gut!**

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, können Sie es sich nach Beantworten einer Sicherheitsabfrage in dakota anzeigen lassen.

Die dakota-Software wird Ihre eingegebenen Informationen ausdrucken. Bitte beachten Sie, dass Sie diesen Ausdruck **nicht** an das 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 und dakota wird Ihre persönlichen Angaben nicht ausdrucken.

2.3.3.4 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 wieder an jede Stelle im Assistenten zurück springen.

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

Konfigurationsassistent 3.2.0.6 für dakota.ag 3.2.0.6

Zertifizierungsantrag
Bitte erfassen Sie Ihre Daten für den Zertifizierungsantrag

Konfiguration

- ✓ Versandart
- Zertifizierungsantrag
- Zertifizierungsantwort

Bei Fragen wenden Sie sich bitte an:

Ihr Logo
Ihr Logo

Vielen Dank für Ihre Angaben! dakota.ag hat nun alle erforderlichen Informationen, um einen Zertifizierungsantrag erstellen zu können.
Bitte kontrollieren Sie noch einmal die nachfolgenden Angaben auf Richtigkeit:

Angaben für den Zertifizierungsantrag:

| | |
|------------------|--------------------|
| Betriebsnummer: | 12345678 |
| Firma: | Musterfirma |
| Ansprechpartner: | Manfred Mustermann |
| Straße: | Musterstraße 23 |
| Ort: | 12345 Musterstadt |
| Tel.-Nr.: | 12345/67890 |
| Fax-Nr.: | 12345/67891 |

Kontrollieren Sie ein letztes Mal Ihre Angaben und bestätigen Sie mit **Weiter >**

Schritt 10 von 11

Abbrechen < Zurück Weiter >

2.3.3.5 Fertigstellen und Aussendung des Schlüssels an das Trust Center

Wenn alle Ihre Angaben korrekt sind, erstellt dakota nun Ihren Schlüssel. Dieser Schlüssel wird per E-Mail an das Trust Center versendet. Zusätzlich druckt dakota für Sie den Antrag auf Zertifizierung aus.

Bitte beachten Sie, dass dieser Antrag auf Zertifizierung vom verantwortlichen Ansprechpartner unterzeichnet werden muss. Wenn dies nicht möglich ist, muss eine formlose Vollmacht des Ansprechpartners dem Antrag auf Zertifizierung beigelegt werden.

Konfigurationsassistent 3.2.0.6 für dakota.ag 3.2.0.6

Zertifizierungsantrag
Bitte erfassen Sie Ihre Daten für den Zertifizierungsantrag

Konfiguration

- ✓ Versandart
- Zertifizierungsantrag
- Zertifizierungsantwort

Bei Fragen wenden Sie sich bitte an:

Ihr Logo
Ihr Logo

dakota.ag erzeugt nun Ihren privaten Schlüssel und versendet die elektronische Zertifizierungsanfrage per E-Mail an das ITSG TrustCenter.

Bitte beachten Sie, dass der Zertifizierungsantrag im Anschluss ausgedruckt wird. Bitte kontrollieren Sie den Ausdruck und korrigieren oder ergänzen Sie diesen ggf. handschriftlich.

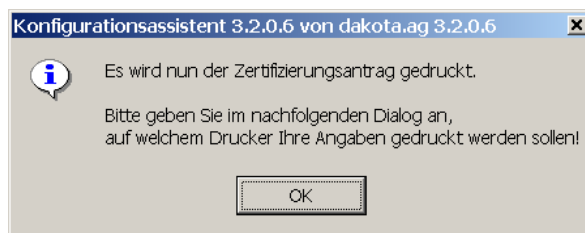
Wählen Sie "Fertigstellen", um den Antrag abzuschließen.

Bestätigen Sie mit **Fertigstellen** um nun den Schlüssel zu erzeugen.

Schritt 11 von 11

Abbrechen < Zurück Fertigstellen

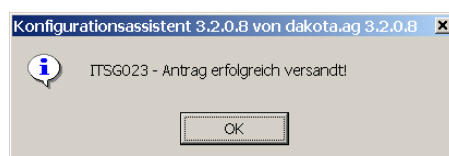
Nachdem der Schlüssel erfolgreich erzeugt ist, wird nun der Schlüssel an das Trust Center per E-Mail oder per HTTPS übertragen und der dazu gehörige Antrag ausgedruckt. Kontrollieren Sie ob Ihr Drucker eingeschaltet ist und bestätigen Sie die folgende Meldung mit **OK**.

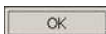



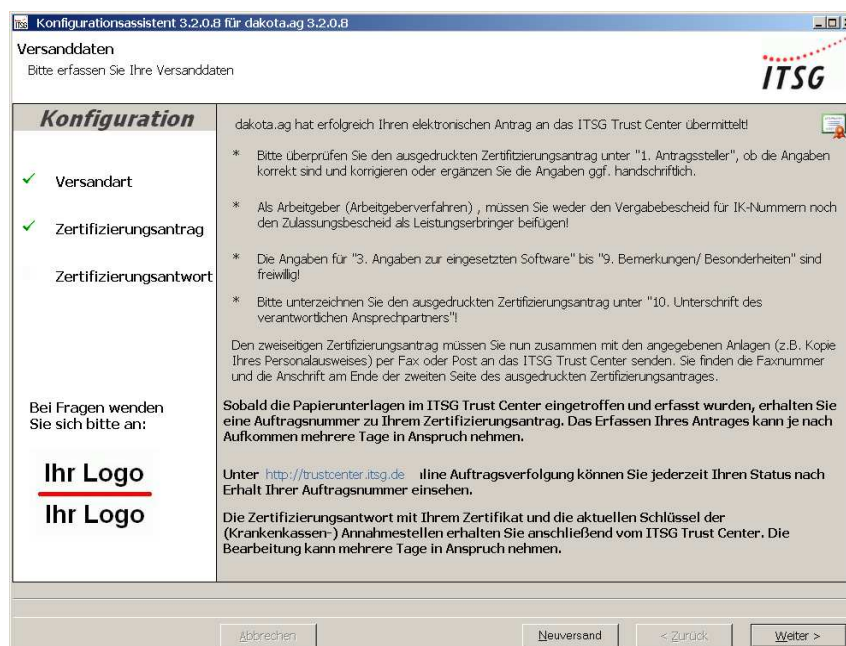
Sollte dieser Dialog nicht erscheinen, so benötigen Sie für diesen Antrag keine Papierunterlagen; Ihr Antrag wurde als Rezertifikat erkannt. Das bedeutet, dass Ihre alten Papierunterlagen für diesen Antrag noch gültig sind.


Sobald Ihr Schlüssel an das Trust Center übertragen wurde, erhalten Sie eine Quittungs-E-Mail. Diese Quittung bedeutet, dass Ihr Schlüssel erfolgreich beim Trust Center empfangen wurde.

Anschließend erhalten Sie folgende Bestätigung, dass der Antrag erfolgreich verschickt wurde:

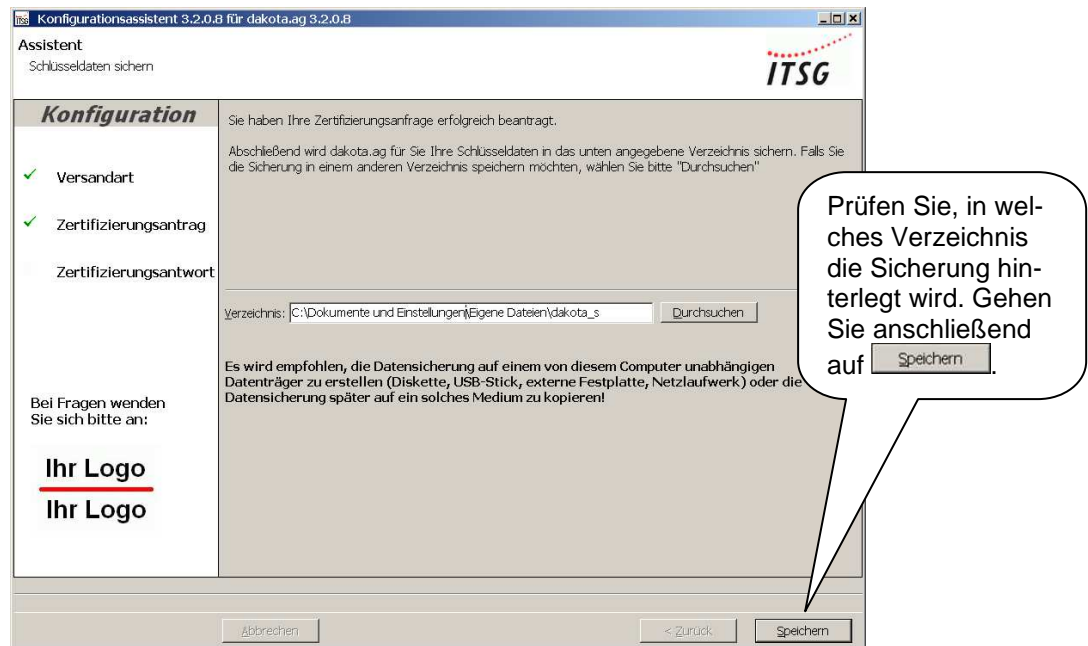


Bestätigen Sie bitte mit  und klicken Sie dann auf . Folgende Maske öffnet sich:



Hinweis: Falls beim Ausdrucken des Antrages für das Trust Center Ihr Drucker nicht funktioniert hat, können Sie mit der Funktion  den Antrag erneut ausdrucken. Auch die E-Mail für das Trust Center wird bei dieser Funktion erneut verschickt.

Wenn alle Schritte durchlaufen sind, erstellt dakota für Ihre Schlüsseldaten einen Sicherungsordner.



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

Wenn Ihr Antrag keine Rezertifizierung ist, so vervollständigen Sie bitte den Papierantrag. Fügen Sie bitte unbedingt eine Kopie des Personalausweises vom verantwortlichen Ansprechpartner hinzu.

In wenigen Tagen werden Sie vom Trust Center eine weitere E-Mail erhalten. In dieser E-Mail wird Ihnen eine **Auftragsnummer** mitgeteilt. 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.

2.3.3.6 Einlesen des Schlüssels vom Trust Center

Nach einer kurzen Bearbeitungszeit von ca. 7 Werktagen erhalten Sie eine weitere E-Mail vom Trust Center. In dieser E-Mail sind Ihr Schlüssel und alle notwendigen Schlüssel der Datenannahmestellen angehängt. Zum Einlesen des Schlüssels bietet Ihnen der Konfigurationsassistent zwei mögliche Schritte:

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

- **Schritt 1: Einlesen des Schlüssels über die Funktion „Abholen“.**
Hierfür stellen Sie bitte Ihre Verbindung zum Internet her und bestätigen Sie anschließend mit .

Zertifizierungsantwort
Bitte lesen Sie die Zertifizierungsantwort ein

Konfiguration

- ✓ Versandart
- ✓ Zertifizierungsantrag
- **Zertifizierungsantwort**

Bei Fragen wenden Sie sich bitte an:
Ihr Logo
Ihr Logo

Sie müssen nun die Zertifizierungsantwort des ITSG Trust Centers einlesen!

Über das Internet vom ITSG Trust Center einlesen
Wenn Sie die Auftragsnummer bereits per E-Mail erhalten haben, geben Sie diese bitte in das Feld "Auftragsnummer" ein. Wenn Sie die Zertifizierungsanfrage über das Internet gestellt haben, ist die Auftragsnummer bereits eingetragen.

Wählen Sie bitte "Abholen" aus, um die Zertifizierungsantwort über das Internet vom ITSG Trust Center zu erhalten.

Auftragsnummer: 123456

Von Datei einlesen
Wenn Sie die Zertifizierungsantwort per E-Mail erhalten haben, können Sie die Dateien "97422004.p7c" und "annahme-pkcs.agv" auch in ein Verzeichnis Ihrer Festplatte speichern (z.B. "C:\dakotaag"). Klicken Sie anschließend "Einlesen" an und wählen Sie die Datei "97422004.p7c" aus.

Datei:

Bitte beachten Sie:
Ihre Auftragsnummer erhalten Sie, sobald Ihre Papierunterlagen im ITSG Trust Center eingetroffen sind und erfasst wurden. Dieser Vorgang kann mehrere Tage dauern.

Unter <http://trustcenter.itsg.de> -> Online Auftragsverfolgung können Sie jederzeit Ihren Status einsehen, sobald Sie Ihre Auftragsnummer per E-Mail erhalten haben oder sich Ihre Zertifizierungsantwort erneut herunterladen.

Schritt 1 von 3

- **Schritt 2: Den Schlüssel über einen Speicherort Ihrer lokalen Festplatte einlesen.** 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.

Zertifizierungsantwort
Bitte lesen Sie die Zertifizierungsantwort ein

Konfiguration

- ✓ Versandart
- ✓ Zertifizierungsantrag
- **Zertifizierungsantwort**

Bei Fragen wenden Sie sich bitte an:
Ihr Logo
Ihr Logo

Sie müssen nun die Zertifizierungsantwort des ITSG Trust Centers einlesen!

Über das Internet vom ITSG Trust Center einlesen
Wenn Sie die Auftragsnummer bereits per E-Mail erhalten haben, geben Sie diese bitte in das Feld "Auftragsnummer" ein. Wenn Sie die Zertifizierungsanfrage über das Internet gestellt haben, ist die Auftragsnummer bereits eingetragen.

Wählen Sie bitte "Abholen" aus, um die Zertifizierungsantwort über das Internet vom ITSG Trust Center zu erhalten.

Auftragsnummer: 123456

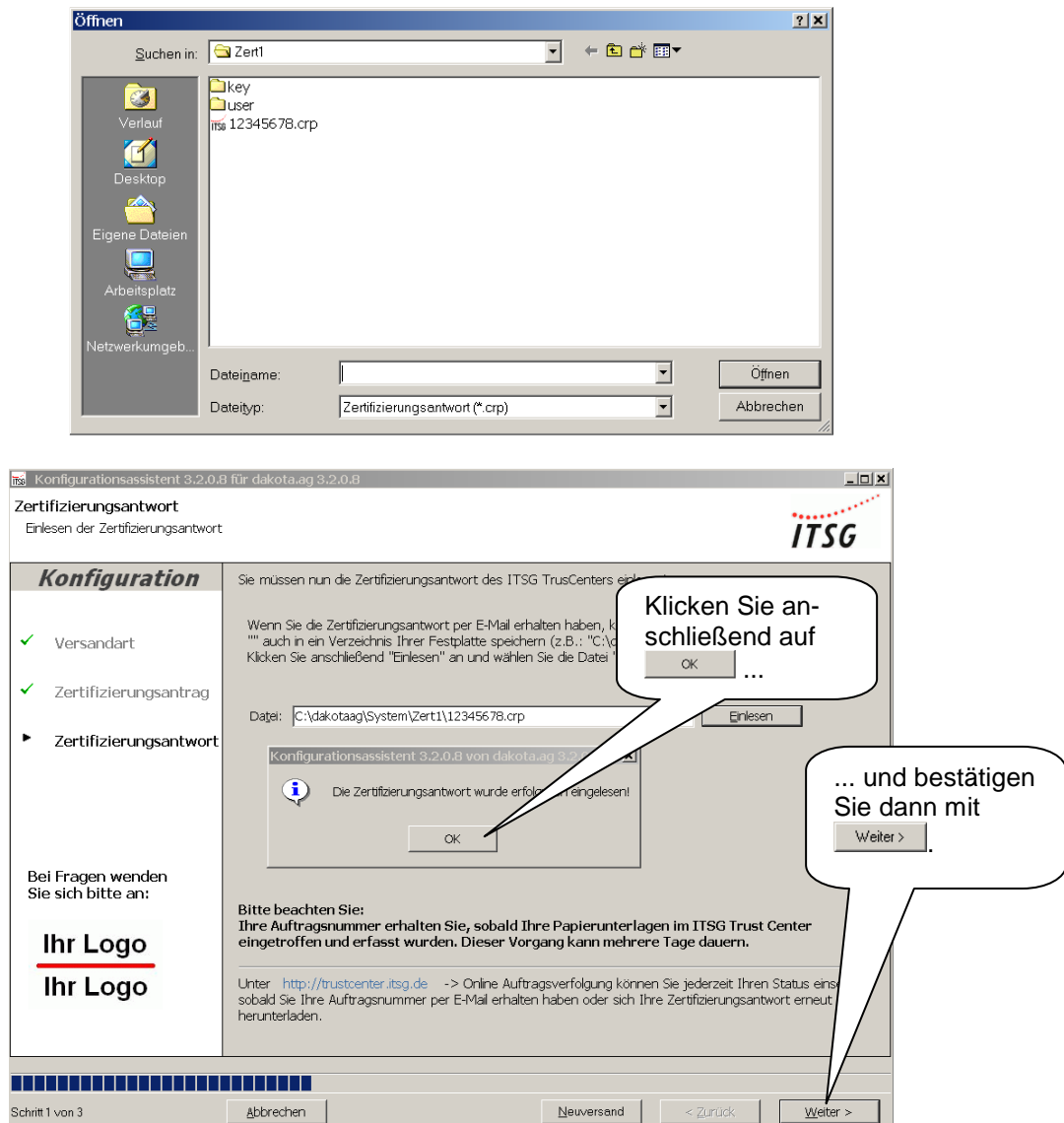
Von Datei einlesen
Wenn Sie die Zertifizierungsantwort per E-Mail erhalten haben, können Sie die Dateien "97422004.p7c" und "annahme-pkcs.agv" auch in ein Verzeichnis Ihrer Festplatte speichern (z.B. "C:\dakotaag"). Klicken Sie anschließend "Einlesen" an und wählen Sie die Datei "97422004.p7c" aus.

Datei:

Bitte beachten Sie:
Ihre Auftragsnummer erhalten Sie, sobald Ihre Papierunterlagen im ITSG Trust Center eingetroffen sind und erfasst wurden. Dieser Vorgang kann mehrere Tage dauern.

Unter <http://trustcenter.itsg.de> -> Online Auftragsverfolgung können Sie jederzeit Ihren Status einsehen, sobald Sie Ihre Auftragsnummer per E-Mail erhalten haben oder sich Ihre Zertifizierungsantwort erneut herunterladen.

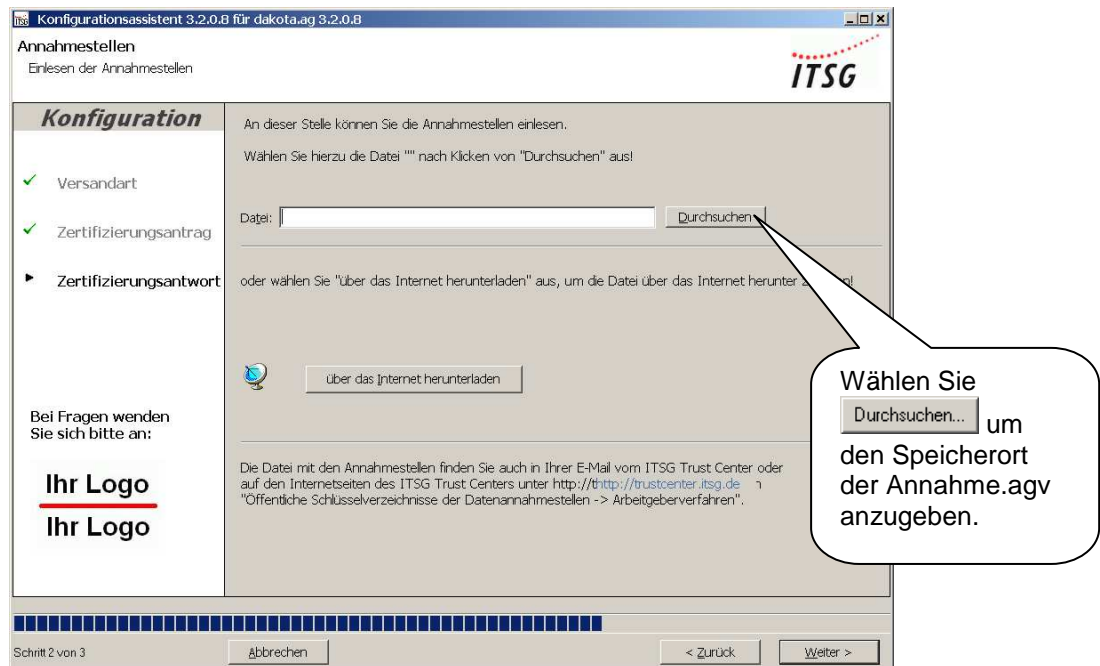
Schritt 1 von 3



Nun müssen Sie noch die Schlüsselliste der Datenannahmestellen einlesen. Hierfür bietet Ihnen der Konfigurationsassistent zwei mögliche Schritte:

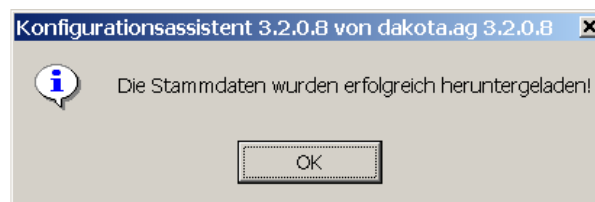
Sie können die Datei `annahme.agv` bzw. `annahme-pkcs.agv` (Arbeitgeberverfahren) oder `annahme.key` bzw. `annahme-pkcs.key` (Leistungserbringerverfahren) ...

- über einen Speicherort Ihrer lokalen Festplatte einlesen.
Wählen Sie hierfür `Durchsuchen...` und geben Sie den Speicherort der Datei **Annahme.agv** / **Annahme-pkcs.agv** oder **Annahme.key** / **Annahme-pkcs.key** ein.

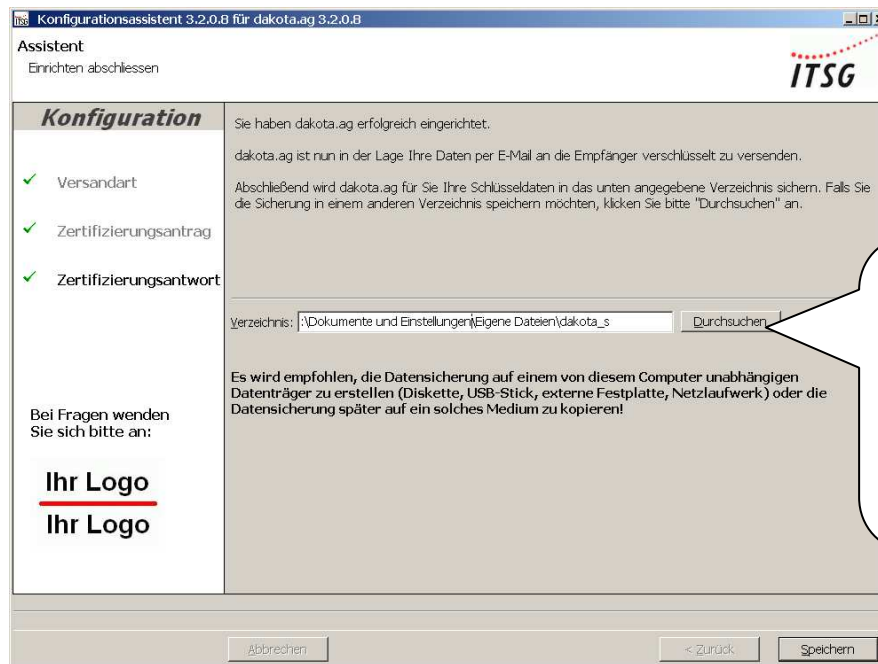


- über das Internet herunterladen und einlesen.
Hierfür öffnen Sie bitte Ihre Verbindung zum Internet und bestätigen Sie diese Funktion mit .

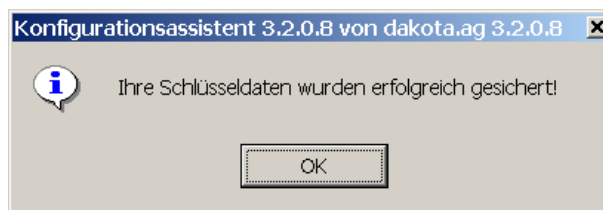
Nachdem das Einlesen erfolgreich abgeschlossen ist, erhalten Sie die folgende Meldung am Bildschirm:



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



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



dakota ist jetzt eingerichtet und bereit, Daten zu verarbeiten. Lesen Sie hierzu weiter im Kapitel 3 Verarbeitung.

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 per E-Mail an die Annahmestellen der Krankenkassen **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 Fehler bei der Verarbeitung auf, werten Sie die Protokolldateien, ggf. mit Ihrem Softwarehaus gemeinsam, aus. Mehr zu den Protokollinformationen finden Sie im Kapitel 4 Protokollierung.

Achtung: Es ist nicht möglich, fehlerhafte Daten per E-Mail abzuschicken. 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 nun per E-Mail verarbeiten 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 → Programme → Dakota → dakota...'.



Abbildung dakota.ag

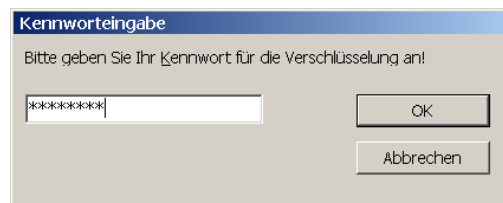
3.3 Daten verarbeiten mit Direktaufruf von dakota

3.3.1 Daten verarbeiten

Beim Daten verarbeiten ist es möglich mit dakota Dateien zu ver- oder entschlüsseln. Für verschlüsselte Daten und unverschlüsselte Daten gibt es getrennte Eingangsverzeichnisse. Bitte beachten Sie das Kapitel 6 Optionen. Dort wird beschrieben, wie Sie die einzelnen Übergabe-verzeichnisse 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 Daten verarbeiten aus.

Beim Verschlüsseln durchsucht dakota - nach der korrekten Passworteingabe - das Verzeichnis `..\Übergabeverzeichnis` auf vorhandene Dateien.



In der nachfolgenden Maske zeigt Ihnen dakota die gefundenen Dateien, die verarbeitet werden, an. Wählen Sie E-Mail und die Daten werden in der von Ihnen eingestellten Versandart versendet. Die aktuell gewählte Versandart wird Ihnen in der Spalte Versandart angezeigt.

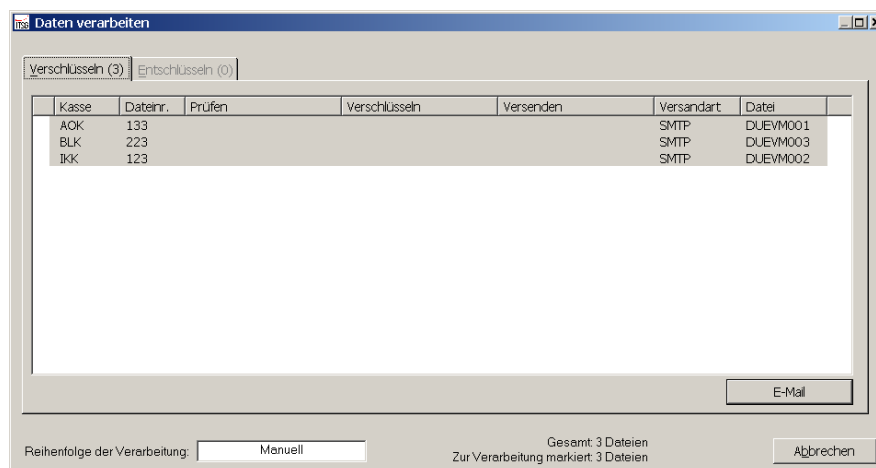


Abbildung dakota.ag

Der Zeitleiste am unteren Rand können Sie die für die dakota-Verarbeitung noch benötigte Zeit entnehmen. Aus dem Vorlaufsatz der Dateien wird von dakota die Kassenart ermittelt, und die erfolgreich geprüfte Datei wird in das Unterverzeichnis dieser Kassenart im Verzeichnis `..\VersandordnerName 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 beim Versenden. Möchten Sie den Vorgang komplett neu starten, weil z. B. die Datei fehlerhaft erzeugt wurde und Sie den gesamten Vorgang neu starten möchten, dann gehen Sie bitte in das Kurzproto-

koll und sehen Sie sich die Details der Verarbeitung an. Das Kurzprotokoll bietet Ihnen umfassende Möglichkeiten zur Administration.

3.3.2 Versenden mit E-Mail: dakota E-Mail

Beachten Sie bitte, dass bei der Versandart dakota E-Mail die Verbindung zum Internet aktiviert sein muss! Wenn Sie die Verbindung nicht manuell vor der Verarbeitung öffnen, kann es zu Fehlern beim Versand kommen.

3.3.3 Versenden mit dem Standard-E-Mail Programm: Outlook Express

Beachten Sie bitte, dass dakota bei dieser Versandart die verschlüsselten Dateien in den Postausgang Ihres genutzten E-Mail-Programms ablegt. Abhängig von den Konfigurationseinstellungen in Ihrem E-Mail-Programm:

- muss die E-Mail von Ihnen aktiv versendet werden oder
- wird die E-Mail ohne Anzeige in MS Outlook-Express verschickt.

Sie müssen ggf. noch die Verbindung ins Internet aufbauen, um die E-Mail(s) zu versenden. Evtl. aufgetretene Fehler beim Versenden per E-Mail werden Ihnen über das Kurzprotokoll von dakota oder über Ihre E-Mail-Software angezeigt.

3.3.4 Versenden mit 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. Zusätzlich werden die zugehörige Auftragssatzdatei und eine Informationsdatei abgelegt. Die Auftragssatzdatei muss zu jeder verschlüsselten Datei beigefügt werden und dient zur genauen Adressierung der verschlüsselten Nutzdaten. Die Informationsdatei enthält alle notwendigen Angaben zum Versand der jeweiligen verschlüsselten Nachricht. Wenn Sie mehr erfahren möchten, lesen Sie bitte im technischen Handbuch die Definition der Informationsdatei nach.

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 und hier **<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.

| Kasse | Dateinummer | Prüfen | Verschlüsseln | Versenden | Versandart | Datei |
|-----------------|---------------|------------------------------------|-----------------------------|----------------------|--------------|-----------------|
| VdAK | 870990 | 09.10.2005 11:32:17 | 09.10.2005 11:32:19 | 09.10.2005 11:32:20 | Email | Tdua0323 |
| Bukn | 12345 | 09.10.2005 11:32:17 | 09.10.2005 11:32:18 | 09.10.2005 11:32:20 | Email | Edua0123 |
| BLK | 314263 | 09.10.2005 11:32:17 | 09.10.2005 11:32:18 | 09.10.2005 11:32:20 | Email | Edua0423 |
| Sonstige | 623142 | 09.10.2005 11:32:17 | Für den Empfänger... | | Email | Edua0426 |
| BKK | 968395 | 09.10.2005 11:32:17 | 09.10.2005 11:32:18 | 09.10.2005 11:32:19 | Email | Tdua0511 |
| AOK | 12345 | 09.10.2005 11:32:17 | 09.10.2005 11:32:18 | 09.10.2005 11:32:19 | Email | Ebnz0223 |
| Bukn | | Verfahrenskennung unbekannt | | | ? | reua0123 |
| VdAK | 870990 | 09.10.2005 11:02:24 | 09.10.2005 11:02:26 | 09.10.2005 11:02:27 | Email | Tdua0323 |
| Bukn | 12345 | 09.10.2005 11:02:24 | 09.10.2005 11:02:26 | 09.10.2005 11:02:27 | Email | Edua0123 |
| BLK | 314263 | 09.10.2005 11:02:24 | 09.10.2005 11:02:26 | 09.10.2005 11:02:27 | Email | Edua0423 |
| BKK | 968395 | 09.10.2005 11:02:24 | 09.10.2005 11:02:25 | 09.10.2005 11:02:26 | Email | Tdua0511 |
| AOK | 12345 | 09.10.2005 11:02:24 | 09.10.2005 11:02:25 | 09.10.2005 11:02:26 | Email | Ebnz0223 |
| ITSG | | | | ITSG023 - Antrag ... | Email | |
| ITSG | | | | ITSG023 - Antrag ... | Email | |

Abbildung dakota.le

Wurden Dateien fehlerfrei verschlüsselt, konnten im Execute-Modus aber nicht versendet werden, können Sie den Sendevorgang für diese Dateien mit **<Daten Versenden>** erneut starten; markieren Sie hierzu die Dateien, die versendet werden sollen. Dies ist z. B. dann der Fall, wenn mittels dakota E-Mail (SMTP-Client) versendet werden sollte, aber die Verbindung zum Internet zum Zeitpunkt des Sendens nicht hergestellt war.

Weitere Informationen zur Auswertung des Kurzprotokolls finden Sie im Kapitel 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. Darüber hinaus können aus dem Kurzprotokoll heraus erfolgreich versendete Dateien erneut (z. B. auf Anforderung des Empfängers) versendet 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 Größe von 64 KB erreicht hat, werden die alten Daten rollierend überschrieben. 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 ebenfalls eine Protokolldatei angelegt, sobald er seinen privaten Schlüssel generiert - 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 geführt. Sie können hier erkennen wann, wie und für welche Annahmestelle Daten geprüft und verschlüsselt wurden. Möchten Sie das Kurzprotokoll aufrufen?

- ⇒ Starten Sie den dakota-Assistenten und wählen hier die Funktion **<Kurzprotokoll>** oder
- ⇒ Starten Sie dakota und wählen Sie aus dem Hauptmenü *'Datei → Kurzprotokoll'*

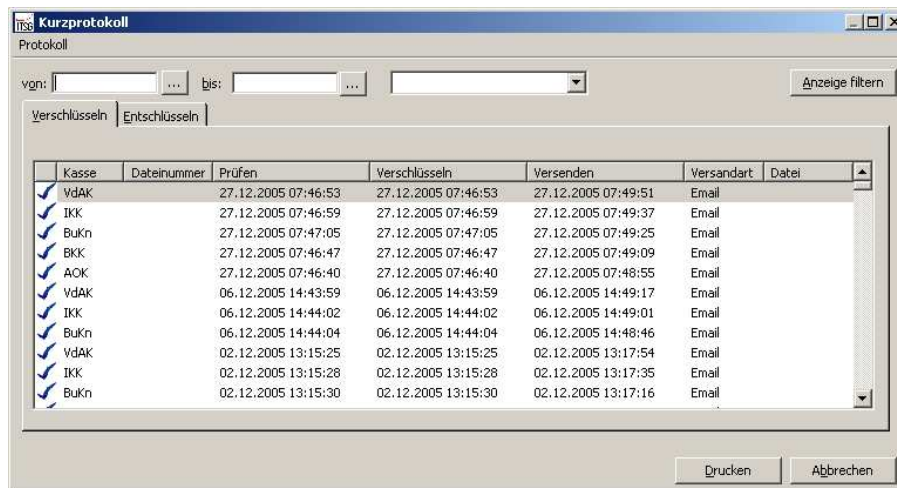


Abbildung dakota.ag

Die einzelnen Spalten lassen sich durch einen Doppelklick in die Spaltenbezeichnung **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 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:

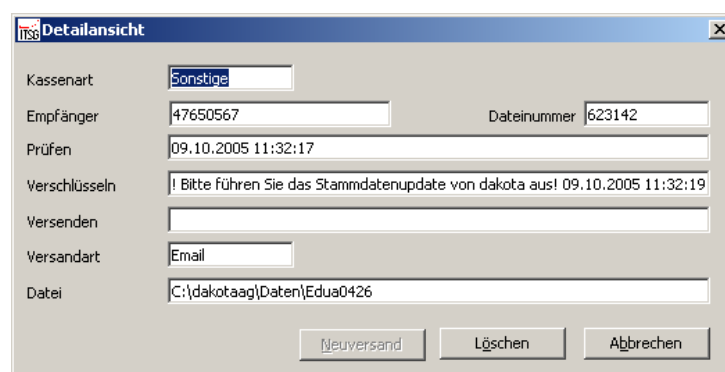



Abbildung dakota.ag

- **Löschen**

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

Hinweis: Bei der Versandart <Standard E-Mail-Programm> werden die erfolgreich gesendeten Nachrichten in Ihrem Standard-E-Mail-Programm gespeichert. Ein Neuversand von erfolgreich gesendeten Nachrichten können Sie in diesem Fall nur über die Archiv-Funktionen Ihres E-Mail-Programms ausführen.

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 Erneuerung Ihres Schlüssels bzw. zum erneuten Einlesen der Schlüssel Ihrer Annahmestellen bereit. Falls Ihr privater (geheimer) Schlüssel einmal defekt oder ‚unsicher‘ werden sollte oder ändert sich der verantwortliche Ansprechpartner in Ihrer Firma, können Sie über den Assistenten einen neuen Schlüssel generieren und damit ein neues Zertifikat beantragen (siehe unter „*Neuer Schlüssel*“).

Die Aktualisierung Ihrer **Annahmestellen** ist ebenso möglich, wenn sich z. B. die E-Mail-Adresse einer Kassenart geändert hat, wie eine Aktualisierung Ihrer Stammdaten per Internet. Öffnen Sie das Menü **<Stammdaten>** und wählen Sie die Funktion **<Stammdatenupdate>** 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 **<Extras> <Sicherung>**.

5.2 Neuer Schlüssel

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 hier 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 Schlüssel defekt und von Ihnen nicht rekonstruierbar (z. B. durch ein Backup)?
- Haben Sie den Verdacht, dass Ihr Schlüssel „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 Trust Center verlängern?

Dann generieren Sie mit dieser Funktion einen neuen privaten Schlüssel.

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

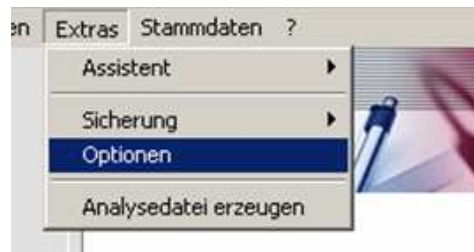
Gehen Sie wie folgt vor:

- ⇒ Starten Sie den **Assistenten** aus Ihrem Anwendungsprogramm oder alternativ aus dem dakota-Hauptmenü **<Extras> <Assistent>**.
- ⇒ Wählen Sie im Assistenten **<Neuen Schlüssel generieren>**.
- ⇒ Sofern ein gültiger Schlüssel vorhanden ist, werden Sie aufgefordert die neue Schlüsselgenerierung zu bestätigen. Bestätigen Sie dies mit **<Ja>**.
- ⇒ Anschließend unterstützt Sie der Assistent bei der Eingabe aller notwendigen Angaben. Bitte sehen Sie hierzu das Kapitel 2.3.3 Konfiguration des Schlüssels (Zertifizierungsantrag).

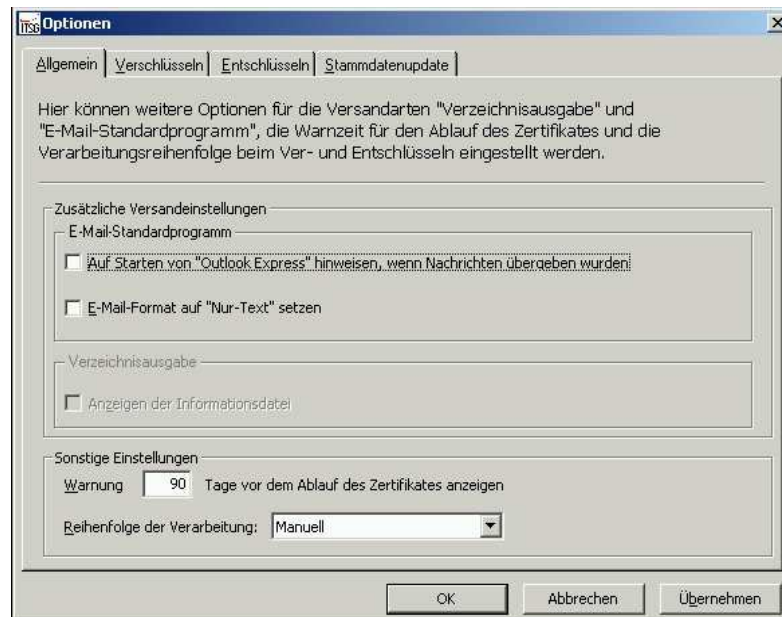
6 Optionen

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

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




6.1 Allgemeine Optionen

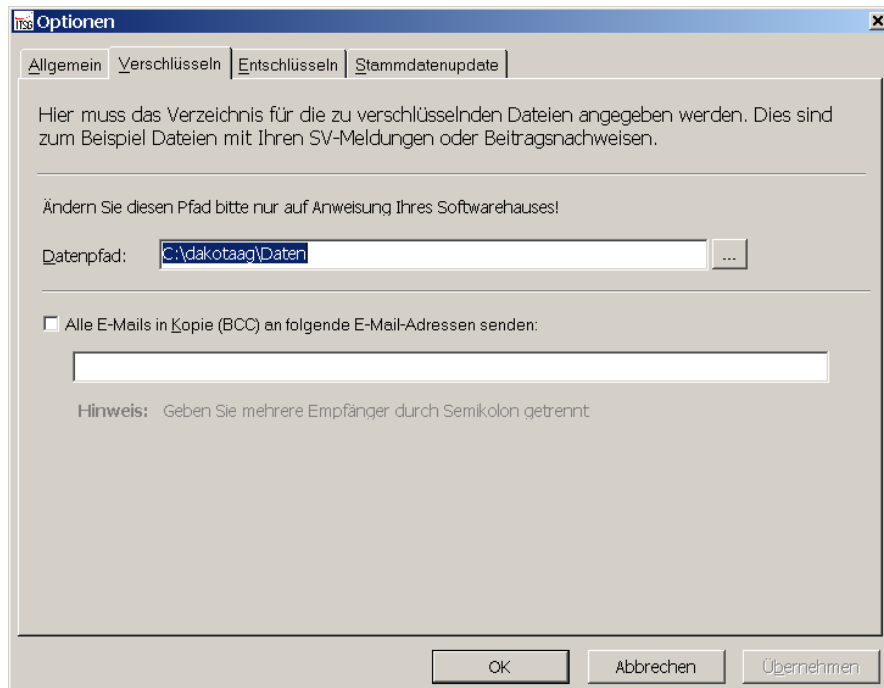


- **Warnung X Tage vor Ablauf des Zertifikates ausgeben.**
Diese Option informiert Sie über das Ablauf Ihres Zertifikates. Standardmäßig ist diese Frist auf 90 Tage eingestellt. Ihr Zertifikat vom Trust Center ist in der Regel 3 Jahre gültig. Der Assistent wird bei jedem Programmstart prüfen, wie lange Ihr Zertifikat noch gültig ist und Sie ggf. mit einer Meldung am Bildschirm informieren. Wenn Ihr Zertifikat abgelaufen ist, müssen Sie einen neuen Schlüssel generieren. Lesen Sie hierzu im Kapitel 5.2 Neuer Schlüssel weiter.
- **Anzeige der Informationsdateien beim Versand als Verzeichnisausgabe**
Bei der Versandart Verzeichnisausgabe können Sie sich die Informationen, die per E-Mail zusätzlich an die Annahmestelle gesendet werden, 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.
- **Reihenfolge der Verarbeitung**
Diese Option bietet Ihnen die Möglichkeit Verarbeitungsabläufe in dakota zu automatisieren. Sie können folgende Optionen angeben:
 - **Verschlüsseln, Entschlüsseln**
Bei dieser Einstellung sucht dakota erst nach den Dateien im Datenpfad, um diese zu verschlüsseln. Im Anschluss sucht dakota automatisch Dateien im Eingangspfad der Entschlüsselung, um diese zu entschlüsseln.
 - **Entschlüsseln, Verschlüsseln**
Bei dieser Einstellung sucht dakota erst nach den Dateien im Eingangspfad der Entschlüsselung, um diese zu entschlüsseln. Im Anschluss sucht dakota automatisch Dateien im Datenpfad, um diese zu verschlüsseln.
 - **Manuell**
Bei dieser Option müssen Sie bei jeder Verarbeitung manuell auswählen, ob Sie zuerst Dateien ent- oder verschlüsseln möchten.

6.2 Optionen für die Verschlüsselung

- **Datenpfad**

Im Datenpfad sucht dakota nach den Abrechnungsdateien, um sie zu verschlüsseln und zu versenden. Wenn Sie den Pfad ändern möchten, können Sie die  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 erhalten sollen.

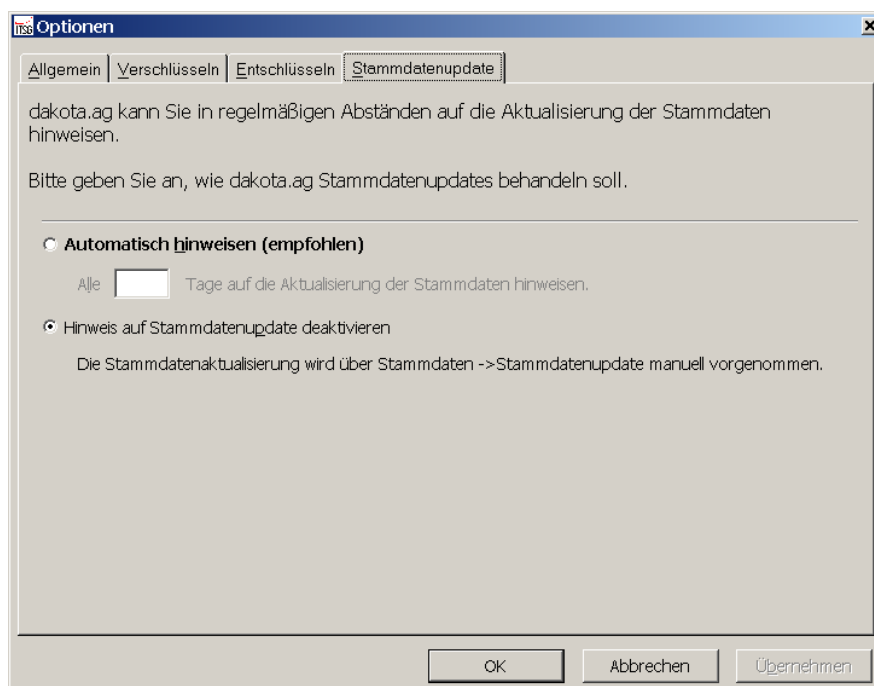
6.3 Optionen für die Entschlüsselung



- **Eingangspfad**
Im Eingangspfad sucht dakota nach verschlüsselten Dateien, um sie zu entschlüsseln. Wenn Sie den Pfad ändern möchten, können Sie dies über diesen Dialog tun. Um den Pfad zu ändern, wählen Sie bitte ...
- **Ausgangspfad**
Im Ausgangspfad speichert dakota die entschlüsselten Dateien nach erfolgreicher Entschlüsselung ab. Wenn Sie den Pfad ändern möchten, können Sie dies über diesen Dialog tun. Um die Pfadangabe zu ändern, wählen Sie bitte ...

6.4 Optionen für das Stammdatenupdate

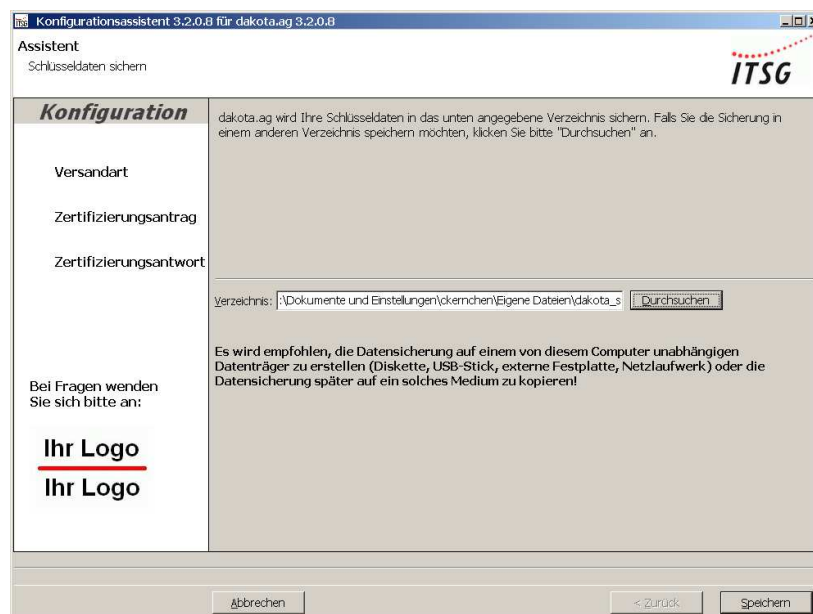
dakota erinnert Sie regelmäßig an die Aktualisierung der Stammdaten der Annahmestellen. Wenn Sie das Update manuell vornehmen möchten und keine Erinnerung wünschen, können Sie die Erinnerungsfunktion abschalten.



6.5 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 wieder herstellen. Wir empfehlen Ihnen in regelmäßigen Abständen Sicherungen anzufertigen und nicht auf der lokalen Festplatte abzulegen. Nutzen Sie ggf. eine CD oder einen anderen Datenträger um die Sicherung aus dem Computer zu exportieren.

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



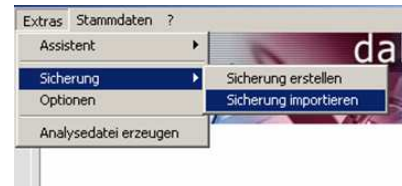
Wählen Sie über die Funktion **Durchsuchen...** ein Verzeichnis, in dem Sie die persönlichen Einstellungen speichern möchten und wählen Sie anschließend **Speichern**.


Die Sicherung wird in dem gewünschten Verzeichnis angelegt. Diese Sicherungsdatei ist mit Tagesdatum und Zeitpunkt der Sicherung benannt.

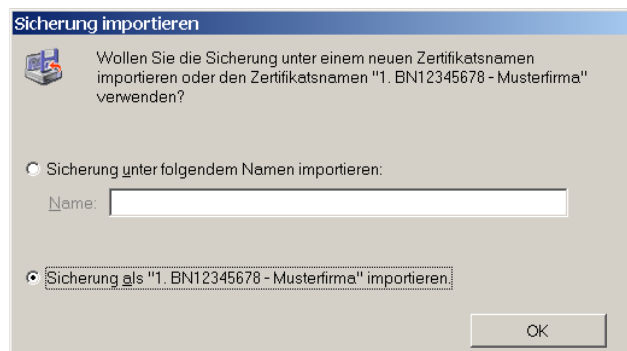
6.6 Sicherung importieren

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

Die Funktion **<Sicherung importieren>** erreichen Sie über die Hauptmaske von dakota, über das Menü **<Extra>** **<Sicherung>** **<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  Sie haben nachfolgend noch die Möglichkeit einen neuen Zertifikatsnamen zu vergeben.



Anschließend importiert dakota die Sicherung und meldet den Erfolg am Bildschirm. Nach dem Import der Sicherung muss die dakota-Software unbedingt neu gestartet werden.



Hinweis: Sie haben auch die Möglichkeit durch einen Doppelklick direkt auf die gewünschte Datei im dakota/s-Ordner das Zertifikat einzulesen.

6.7 Eigene Schlüsseldaten

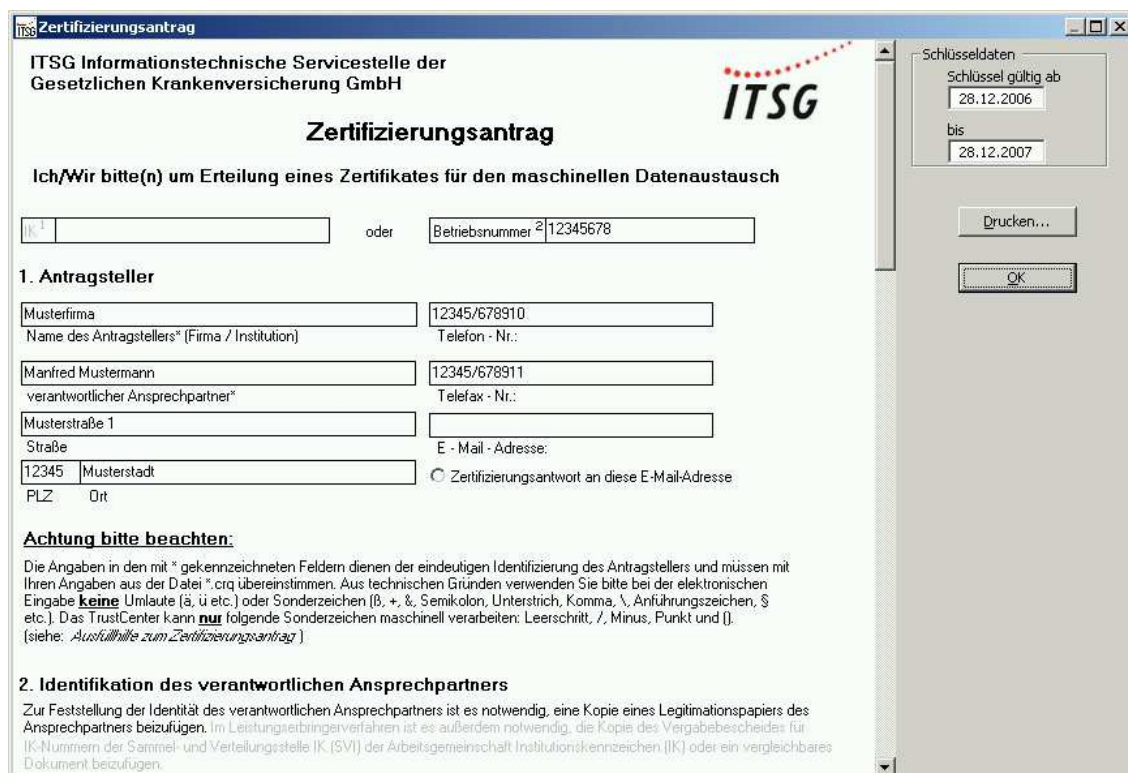
Die Informationen bezüglich Ihres eigenen Schlüssels können Sie jederzeit in der dakota-Software einsehen. Sie finden Ihre Eingaben über die Funktion **<Eigene Schlüsseldaten>**.

Wählen Sie hierfür auf der Hauptmaske von dakota das Menü **<Stammdaten>** und anschließend die Funktion **<Eigene Schlüsseldaten>**



Die Maske **<Eigene Schlüsseldaten>** bietet Ihnen noch weitere Informationen und Möglichkeiten. Sie können am oberen rechten Rand des Bildschirms erkennen, wie lange Ihr eigener Schlüssel noch gültig ist. Sie können gerne diese Ansicht über Ihren Drucker auf Papier ausdrucken. Wählen Sie hierfür **Drucken...** und folgen Sie dem Dialog.

Zum Verlassen dieser Maske wählen Sie bitte **OK**.



ITSG Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH

Zertifizierungsantrag

Ich/Wir bitte(n) um Erteilung eines Zertifikates für den maschinellen Datenaustausch

IK¹ oder Betriebsnummer²

1. Antragsteller

Musterfirma
Name des Antragstellers* (Firma / Institution) Telefon - Nr.:

Manfred Mustermann
verantwortlicher Ansprechpartner* Telefax - Nr.:

Musterstraße 1
Straße E - Mail - Adresse:

PLZ Ort ☐ Zertifizierungsantwort an diese E-Mail-Adresse

Achtung bitte beachten:

Die Angaben in den mit * gekennzeichneten Feldern dienen der eindeutigen Identifizierung des Antragstellers und müssen mit Ihren Angaben aus der Datei *.crq übereinstimmen. Aus technischen Gründen verwenden Sie bitte bei der elektronischen Eingabe **keine** Umlaute (ä, ü etc.) oder Sonderzeichen (ß, +, &, Semikolon, Unterstrich, Komma, \, Anführungszeichen, \$ etc.). Das TrustCenter kann **nur** folgende Sonderzeichen maschinell verarbeiten: Leerschritt, /, Minus, Punkt und {}.

(siehe: *Ausfüllhilfe zum Zertifizierungsantrag*)

2. Identifikation des verantwortlichen Ansprechpartners

Zur Feststellung der Identität des verantwortlichen Ansprechpartners ist es notwendig, eine Kopie eines Legitationspapiers des Ansprechpartners beizufügen. Im Leistungserbringungsverfahren ist es außerdem notwendig, die Kopie des Vergabebescheides für IK-Nummern der Sammel- und Verteilungsstelle IK (SVI) der Arbeitsgemeinschaft Institutionskennzeichen (IK) oder ein vergleichbares Dokument beizufügen.

Schlüsseldaten

Schlüssel gültig ab
bis

Drucken...

OK

6.8 Erweiterte SMTP Optionen

Die Versandart SMTP bietet Ihnen noch erweiterte Konfigurationseinstellungen. Je nachdem wie performant Ihre Internetverbindung ist, müssen Sie ggf. die folgenden Einstellungen anpassen:

Hinweis: Bevor Sie diese Option ändern oder anpassen, sprechen Sie bitte mit Ihrem Systemadministrator oder Ihrem Softwarebetreuer.

- **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.
- **Anzahl der Sendeversuche**
Die Anzahl der Sendeversuche zum SMTP-Server beträgt standardgemäß 1. Die Anzahl muss ggf. erhöht werden, wenn die Reaktionszeit des angesprochenen SMTP-Servers zu lang ist.
- **Servertimeout**
Das sog. Servertimeout ist die Zeitspanne zwischen den Versuchen eine Verbindung zum SMTP-Server aufzubauen. Die Anzahl muss ggf. erhöht werden, wenn die Reaktionszeit des angesprochenen SMTP-Servers zu lang ist.

Konfigurationsassistent 3.2.0.8 für dakota.ag 3.2.0.8

Versanddaten
Bitte erfassen Sie Ihre Versanddaten

Konfiguration

Sie möchten die E-Mails direkt über das Internet versenden. Hierfür benötigt dakota.ag noch die folgenden Angaben

► Versandart

- ✓ Zertifizierungsantrag
- ✓ Zertifizierungsantwort

Bei Fragen wenden Sie sich bitte an:

Ihr Logo
Ihr Logo

ITSG

Allgemein Erweitert

Anschlussnummer (Port) des Postausgangsservers (SMTP): Standard verwenden

Anzahl der Sendeversuche:

Servertimeout

Kurz Lang 10 Sekunden

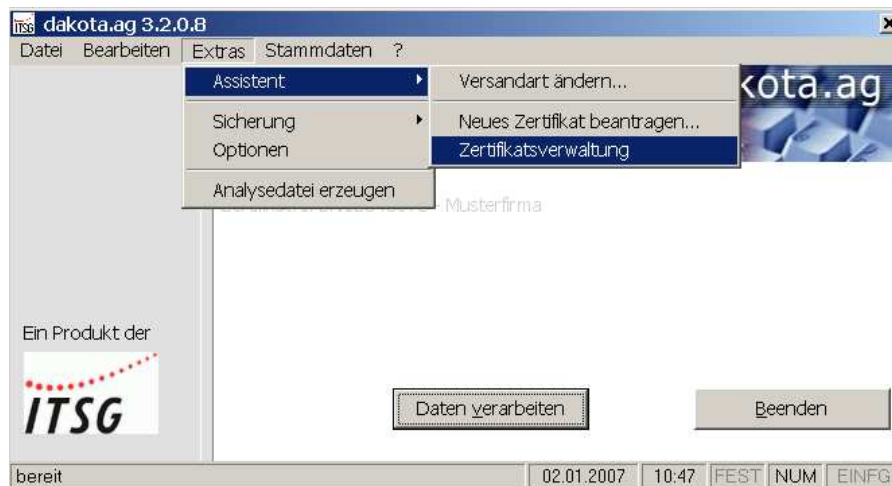
Schritt 2 von 4 Abbrechen < Zurück Weiter >

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

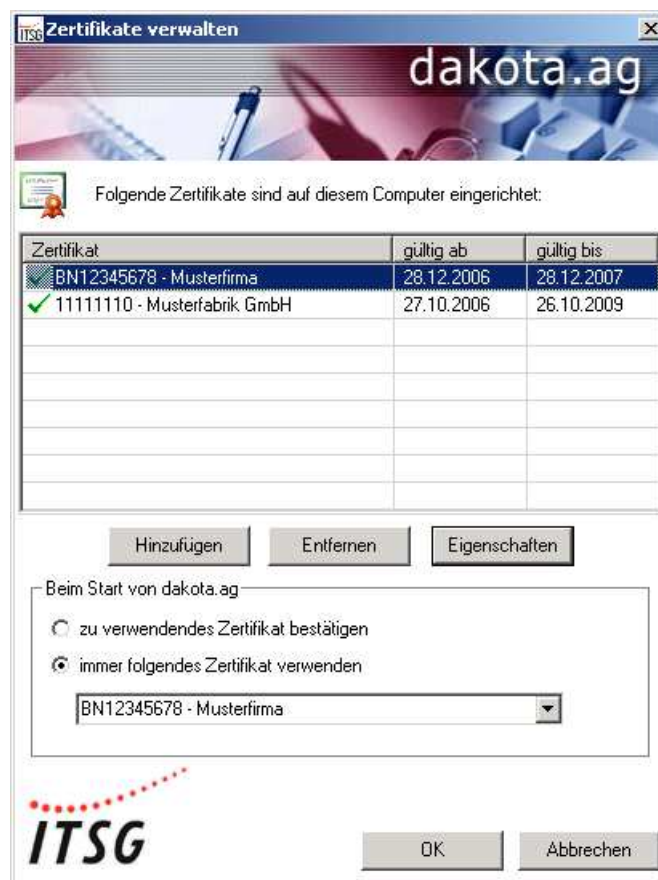
6.9 Zertifikatsverwaltung

Mit Hilfe der Zertifikatsverwaltung können Sie Ihre Schlüssel in dakota verwalten.

Die Funktion **<Zertifikatsverwaltung>** erreichen Sie über die Hauptmaske von dakota, über das Menü **<Extra> <Assistent> <Zertifikatsverwaltung>**.

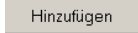


Folgendes Fenster öffnet sich:




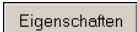
Um ein Zertifikat nur für die laufende Sitzung zu wechseln, wählen Sie dieses bitte aus, klicken Sie auf **OK** und bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Auf dem unteren Teil der Maske können Sie das Standard-Zertifikat, welches automatisch bei jedem Programmstart gewählt wird, festlegen.

Über die Funktion  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 6.6 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.

Über  können Sie sich die erweiterten Informationen zu Ihrem ausgewählten Zertifikat anzeigen lassen.

7 Häufig gestellte Fragen

7.1 Allgemeine Fragen zu dakota^{ag}

- **Wo kann ich Informationen über den elektronischen Datenaustausch mit den Krankenkassen erhalten?**

Die rechtlichen und technischen Vorgaben für die Übermittlung elektronischer Daten an die Krankenkassen finden Sie im Internet unter www.gkv-ag.de und www.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 3 Jahren und kann nach Ablauf nicht weiter verwendet werden.

- **Wann muss ich mein Zertifikat vom Trust Center verlängern?**

Das Zertifikat hat eine begrenzte Laufzeit von drei Jahren. dakota^{ag} warnt Sie vor dem Ablauf dieses Zeitraumes (z. B. 90 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 gesetzlichen Krankenkassen erstellen alle 3 Jahre einen neuen Schlüssel. Der nächste Schlüsselwechsel findet am 31.12.2007 statt. Dadurch ist eine Aktualisierung der öffentlichen Schlüsseldatei (annahme.agv bzw. 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 erhalte ich die Zulassung zur DEÜV?**

Melden Sie sich bei einer Krankenkasse für die Zulassung zum automatisierten Meldeverfahren an. Diese Zulassung gilt dann für alle Krankenkassen.

- **Wie finde ich die Betriebsnummern der Krankenkassen?**

Informationen über alle Betriebsnummern der Krankenkassen finden Sie unter www.gkv-aq.de. Dort können Sie auch eine Betriebsnummerndatei herunterladen.

7.2 Allgemeine Fragen zu dakota^{le}

- **Wo kann ich Informationen über den elektronischen Datenaustausch mit Krankenkassen erhalten?**
Die rechtlichen und technischen Vorgaben für die Übermittlung elektronischer Daten an die Krankenkassen finden Sie unter <http://www.itsg.de> und <http://www.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 weiter verwendet werden.
- **Wann muss ich mein Zertifikat vom Trust Center verlängern?**
Das Zertifikat hat eine begrenzte Laufzeit von drei Jahren. dakota^{le} warnt Sie vor dem Ablauf dieses Zeitraumes (z. B. 90 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 gesetzlichen Krankenkassen erstellen alle 3 Jahre einen neuen Schlüssel. Der nächste Schlüsselwechsel findet am 31.12.2007 statt. Dadurch ist eine Aktualisierung der öffentlichen Schlüsseldatei (annahme.key bzw. 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.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.

- **Wie werden E-Mail-Programme von dakota angesprochen?**

dakota ist für den automatischen E-Mail-Versand mit Microsoft Outlook Express entwickelt worden. Die Erzeugung einer E-Mail in dakota wird über die MAPI oder CDO Schnittstelle von Windows realisiert. Daher können alle E-Mail-Programme, die die MAPI Schnittstelle unterstützen, von dakota genutzt werden. Der Einsatz von anderen E-Mail-Programmen als MS Outlook Express muss durch eigene Tests sichergestellt werden.

- **Welche Internet-Provider unterstützt dakota?**

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

- **Wie konfiguriere ich mein T-Online?**

Richten Sie in MS Outlook Express ein Konto für E-Mail ein, die Kontobezeichnung ist Ihre Betriebs- bzw. Ihre IK-Nummer. Für die automatische Anwahl zu T-Online muss ein neuer Internetzugang erzeugt werden, nutzen Sie dafür bitte die Windows Assistenten. Der Kontoname, der für den Internetzugang gefordert ist, setzt sich bei T-Online aus Ihrer Anschlusskennung, der T-Online Telefonnummer und dem Suffix zusammen (Beispiel: 00012345678902211234567#0001).

- **Wie konfiguriere ich mein T-Online mit Outlook Express?**

Um mit Outlook Express über den Provider T-Online E-Mails versenden zu können, muss zunächst eine DFÜ-Verbindung eingerichtet werden. Es ist leider nicht möglich die bestehenden Einwahlverbindungen, die das so genannte "StartCenter" schafft, zu nutzen. Im zweiten Schritt wird das E-Mail-Konto in Outlook Express für den Versand mit T-Online eingerichtet.

- **DFÜ-Netzwerk-Verbindung mit T-Online**

Sie müssen bei einem T-Online-Zugang zuerst eine reine PPP-Verbindung mittels des DFÜ-Netzwerks von Windows aufbauen.

Öffnen Sie dafür über das **Startmenü → Einstellungen** den Ordner **<Netzwerk- und DFÜ-Verbindungen>**.

Doppelklicken Sie dann auf **<Neue Verbindung erstellen>**.

Geben Sie nun einen beliebigen Namen für die neue Verbindung ein, zum Beispiel "T-Online". Wählen Sie darunter Ihr Modem für den Internet-Zugang aus und klicken Sie auf **<Weiter>**.

Geben Sie als Rufnummer die bundeseinheitliche Nummer **<0191011>** ein. Das Feld **<Ortskennzahl>** können Sie leer lassen. Klicken Sie anschließend auf **<Weiter>** und dann auf **<Fertig stellen>**.

Klicken Sie mit der rechten Maustaste auf die neue Verbindung. Wählen Sie **<Eigenschaften>** und entfernen Sie den Haken vor **<Ortskennzahl und Wählparameter verwenden>**. Wechseln Sie zur Karte **<Netzwerk>**. Überprüfen Sie, dass nur vor **<Softwarekomprimierung aktivieren>** und **<TCP/IP>** Haken sind und klicken Sie dann auf **<OK>**.

Doppelklicken Sie nun auf die neue DFÜ-Verbindung. Unter **<Benutzername>** tragen Sie Ihre zwölfstellige Anschlusskennung (A), Ihre T-Online-Nummer (T), eine Raute (#) und die Mitbenutzernummer (M) ein. Ist Ihre

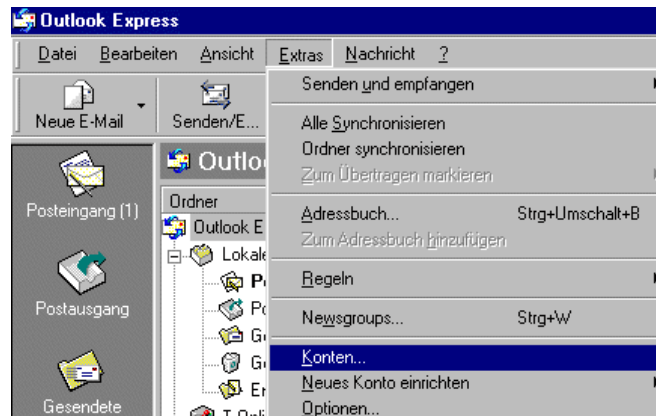
- Anschlusskennung "000123456789",

- Ihre T-Nummer "0211998877",
 - und Ihre Mitbenutzernummer "0001",
- tragen Sie also "0001234567890211998877#0001" ein.
Bei **<Kennwort>** fügen Sie Ihr T-Online-Kennwort ein. Setzen Sie ein Häkchen vor die Option **<Kennwort speichern>** (wenn gewünscht), und klicken Sie auf **<Verbinden>**.

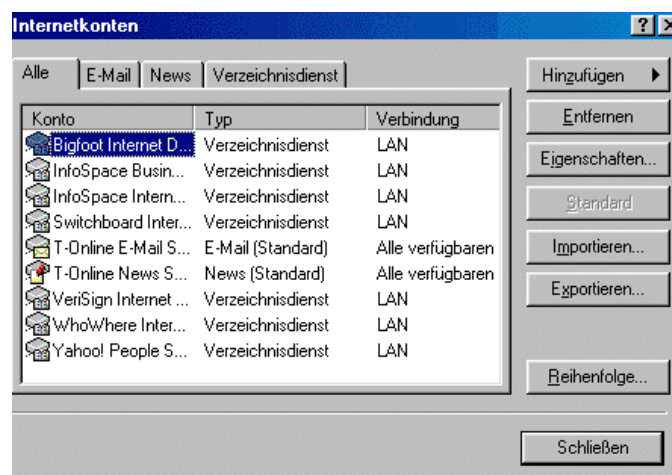
- **E-Mail-Konto für T-Online mit Outlook Express einrichten**

Nachdem nun die DFÜ Verbindung zu T-Online eingerichtet ist, müssen noch die Anmeldeinformationen für das E-Mail-Konto in Outlook Express eingetragen werden.

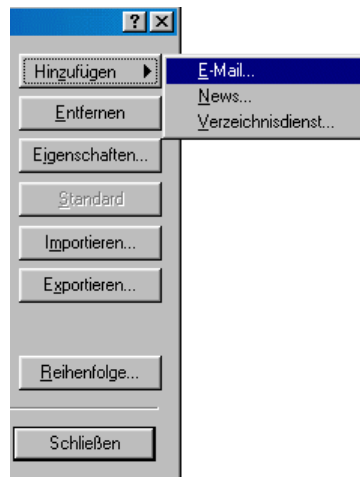
Um das Microsoft E-Mail-Programm zu konfigurieren, starten Sie Outlook Express. Rufen Sie im Menü **<Extras>** den Menüpunkt **<Konten>** auf.



Wählen Sie im Menü **<Internetkonten>** nun den Menüpunkt **Hinzufügen**.



Gehen Sie dann auf den Unterpunkt **<E-Mail>**.



Es wird der **<Assistent für den Internetzugang>** gestartet. Tragen Sie im Feld **Name** bitte Ihren Vor- und Nachnamen ein und bestätigen Sie mit **>Weiter<**.

 A screenshot of the 'Assistent für den Internetzugang' (Internet Connection Wizard) dialog box. The title bar says 'Assistent für den Internetzugang'. The main heading is 'Ihr Name'. Below it, there is a text box for 'Name:' containing 'Vorname Nachname'. A note above the text box says: 'Wenn Sie eine Nachricht senden, erscheint Ihr Name in dem "Von" Feld der Nachricht. Geben Sie Ihren Namen so ein wie er erscheinen soll.' Below the text box is an example: 'Beispiel: Jens Mander'. At the bottom are three buttons: '< Zurück', 'Weiter >', and 'Abbrechen'.

Tragen Sie im Feld **E-Mail-Adresse** bitte Ihre komplette E-Mail-Adresse ein und bestätigen Sie die Eingabe mit **Weiter >**

 A screenshot of the 'Assistent für den Internetzugang' dialog box, showing the 'Internet E-Mail Adresse' step. The title bar says 'Assistent für den Internetzugang'. The main heading is 'Internet E-Mail Adresse'. Below it, there is a text box for 'E-Mail-Adresse:' containing 'vorname.nachname@t-online.de'. A note above the text box says: 'An Sie gerichtete E-Mail-Nachrichten werden an Ihre E-Mail-Adresse geleitet.' Below the text box is an example: 'Zum Beispiel: jemand@microsoft.com'. There are two radio buttons: the first is selected and labeled 'Ich habe bereits eine E-Mail-Adresse.', and the second is labeled 'Neues Konto einrichten bei:'. At the bottom are three buttons: '< Zurück', 'Weiter >', and 'Abbrechen'.

Tragen Sie nun als Posteingangsserver POP.T-ONLINE.DE und als Postausgangsserver (SMTP) MAILTO.T-ONLINE.DE ein. Bestätigen Sie Ihre Eingabe mit **Weiter >**.

Assistent für den Internetzugang

Namen der E-Mail-Server

Mein Posteingangsserver ist ein **POP3** Server.

Posteingangsserver (POP3, IMAP oder HTTP):

Ein SMTP Server wird für den Postausgang verwendet.
 Postausgang (SMTP):

< Zurück Weiter > Abbrechen

Outlook Express verlangt die Eingabe von Kontoname und Kennwort. (T-Online wertet diese Angaben jedoch nicht aus, da die Identifikation bereits bei der Einwahl mit Ihren T-Online Zugangsdaten erfolgt.) Als Kontoname empfehlen wir, Ihren E-Mail-Alias oder Ihre T-Online-Nummer einzugeben. Im Feld **Kennwort** geben Sie aus Sicherheitsgründen bitte nicht Ihr T-Online-Kennwort ein, sondern lediglich einen Punkt (".") Bestätigen Sie die Eingabe mit **Weiter >**.

Assistent für den Internetzugang

Internet E-Mail Anmeldung

Geben den Kontonamen und das Kennwort ein, die Sie von Ihrem Internetdienstanbieter erhalten haben.

Kontoname:

Kennwort:

☒ Kennwort speichern

Wenn Ihr Internetdienstanbieter gesicherte Kennwort-Authentifizierung (SPA) für den Zugriff auf das E-Mail-Konto unterstützt, aktivieren Sie das Kontrollkästchen "Anmeldung durch gesicherte Kennwort-Authentifizierung (SPA)".

☐ Anmeldung durch gesicherte Kennwort-Authentifizierung (SPA)

< Zurück Weiter > Abbrechen

Um die Konfiguration abzuschließen und die Einstellungen zu speichern, bestätigen Sie mit **Fertig stellen**.

Assistent für den Internetzugang

Installation beendet

Alle Informationen zur Einrichtung des gewünschten Kontos wurden vollständig eingegeben.

Um diese Einstellungen zu speichern, klicken Sie auf "Fertig stellen".

< Zurück **Fertig stellen** Abbrechen

- **Welche Systemrechte benötige ich bei Windows 2000?**
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 <Optionen> das Online Stammdatenupdate.
- **Wie kann ich den Trust Center-Antrag noch einmal ausdrucken?**
Sie haben die Möglichkeit, den Antrag noch einmal auszudrucken, indem Sie beispielsweise beim Einlesen der Zertifizierungsantwort die Funktion <Neuversand> wählen. Sie können ebenfalls über die Hauptmaske von dakota über das Menü <Stammdaten> <Eigene Schlüsseldaten> den Antrag erneut ausdrucken. Wählen Sie hierfür <Drucken> und folgen Sie dem Dialog.
- **Wie verarbeite ich die E-Mail vom Trust Center mit meinem Zertifikat?**
Vom Trust Center erhalten Sie eine E-Mail mit 3 Anhängen, Ihrem Zertifikat (anwender.crp bzw. anwender.p7c), der öffentlichen 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 Trust Center erhalten Sie eine E-Mail mit einem Anhang oder Sie kopieren die Datei von der ITSG Homepage <http://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.
- **Die Annahmestellen melden, dass Anhänge fehlen. Was tun?**
Beim Einsatz von MS Outlook kann es passieren, dass ein eigenes Format von Microsoft die 2 notwendigen Anhänge zusammenfasst und die Annahmestellen diese E-Mails nicht verarbeiten können. In MS Outlook muss sichergestellt sein, das als E-Mail-Format **<Nur Text>** eingestellt wird, ein evtl. vorhandener MS Exchange Server darf diese Einstellung nicht verändern.
- **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.
- **Welche E-Mail Systeme kann ich mit dakota verwenden?**
Es liegen positive Meldungen vor, dass die folgenden E-Mail Programme problemlos eingesetzt werden können. Eine Garantie kann dafür aber nicht übernommen werden! „*Messenger von Netscape*“, „*MS Outlook 97/98*“, „*MS Outlook 2000*“, „*MS Outlook XP*“, „*MS Outlook 2003*“, „*eudora*“, „*Lotus Notes*“

8 Änderungshistorie

In diesem Abschnitt werden die Änderungen zu den Vorversionen des Handbuches dokumentiert. Sie können an Hand der folgenden Tabelle die Änderungen in den Kapiteln ab der Version 3.0 nachvollziehen.

| Kapitel | Titel | Seitenzahl |
|---------|--|------------|
| 2.3.3.1 | Beim Erfassen der Adressdaten werden Sonderzeichen, wie ä, ö, ü, etc. automatisch in ae, oe, ue, etc. umgewandelt. | 17 |
| 2.3.3.2 | Beim Erfassen des verantwortlichen Ansprechpartners werden Sonderzeichen, wie ä, ö, ü, etc. automatisch in ae, oe, ue, etc. umgewandelt. | 18 |
| 2.3.3.5 | Nach erfolgreicher Schlüsselerzeugung kann nun der Schlüssel an das Trust Center nicht nur per E-Mail oder auch per HTTPS übertragen werden. | 20 |
| 2.3.3.5 | Bei der Fertigstellung und Aussendung des Schlüssels an das Trust Center ist ein Papierantrag für Rezertifizierer nicht mehr notwendig. | 21 |
| 2.3.3.6 | Zum Einlesen des Schlüssels vom Trust Center gibt es nun auch eine zweite Möglichkeit. Über den Button „Abholen“ wird die Zertifizierungsantwort beim Trust Center automatisch abgeholt und verarbeitet. | 23 |

9 Index

A

Abrechnungsverfahren
 maschinell 5, 51
Aktualisierung 36
Annahmestelle 27, 32, 49, 51, 56
Assistent 10

C

CDO-Schnittstelle 52
Copyright 2

D

dakota 4
digitale Signatur 5

E

Einleitung 4
E-Mail-Alias 55
Execute-Modus 10, 31, 33

F

Fachanwendung 27, 28, 31

G

geheimer Schlüssel 5

I

Inbetriebnahme 6

K

kryptographisches Verfahren 5
Kurzprotokoll 27, 31, 32, 34

L

Langprotokoll 33
Laufzeit 36, 49, 51

M

MAPI-Schnittstelle 52

Microsoft 2

N

neuer Schlüssel 37

O

öffentlicher Schlüssel 5, 49, 51
Outlook Express 30

P

Passwort 29
privater Schlüssel 5
Programmstart 10, 28
Protokollierung 32

R

rollierende Logdatei 33

S

Schlüsselgenerierung 32, 37
Schlüsselpaar 5
Schnittstelle 52
Sicherheitsverfahren 5
SMTP-Client 31
Systemcrash 56

T

TrustCenter 5, 37, 56

V

Verarbeitung 27
Verschlüsseln und Versenden integriert in die
 Fachanwendung 31
versenden
 mit E-Mail
 dakota E-Mail 30
 Outlook Express 30
 mit Fremd-EMail - Verzeichnis Ausgabe 30

Z

Zertifikat 5, 36, 37, 49, 51
Zertifizierungsantrag 37