[michael martin]
UNTERNEHMENSGRUPPE
☎ 06227-8383-83 Fax: 06227-8383-99

mmOrthosoft®

Seminar

§300 / §302 SGB V

Einrichtung DAKOTA.LE Verschlüsselungssoftware

Ausgabedatum 29.04.2020

Sehr geehrte Anwender,

unsere Branche steht vor großen Herausforderungen. Hoher Wettbewerbsdruck, sinkende Erlöse und ständige Veränderungen im Gesundheitswesen sprechen eine deutliche Sprache. Um Ihren Unternehmenserfolg zu sichern, müssen Sie sich noch intensiver um Ihre Kunden bemühen.

Dies wird erreicht, indem man andere Bereiche wie die aufwändige Verwaltung noch mehr strafft. Als Anbieter einer echten Branchenlösung bieten wir getreu unserem Motto:

...viel mehr als nur Software !

Lösungen für alle Verwaltungsbereiche an. Basierend auf dem Kostenvoranschlag, bis hin zur kompletten Abrechnung, über den Einsatz zeitsparender Büroprogramme wie Termin- und Zeitplanung, bis hin zu einem integrierten elektronischen Qualitätsmanagement Handbuch.

Oft wird nur ein kleiner Teil der vorhandenen Möglichkeiten ausgeschöpft. Mit diesem Seminar zeigen wir Ihnen, wie Sie Ihre Software noch effektiver nutzen.

Sie werden feststellen, dass Sie das Gelernte binnen kurzer Zeit zum Vorteil Ihres Unternehmens einsetzen können.

Wir wünschen Ihnen dabei viel Erfolg.

Das ganze mm-Team mit der Geschäftsleitung

Carmen & Michael Martin

1 Inhaltsverzeichnis

Index

2 Einführung

Der Gesetzgeber hat bereits 1992 im Rahmen des Gesundheitsstrukturgesetzes die Krankenkassen verpflichtet, zukünftig Leistungen nur noch dann zu vergüten, wenn die Abrechnung auf maschinenlesbaren oder maschinell verwertbaren Datenträgern erfolgt. Die entsprechenden Vorschriften sind für die „sonstigen Leistungserbringer“ in den §300, § 302 und § 303 des fünften Sozialgesetzbuches (SGB V) geregelt.

Ziel der Einführung des maschinellen Abrechnungsverfahrens zwischen den Krankenkassen und den Leistungserbringern ist die Nutzung zeitgemäßer Kommunikationstechniken und die bundesweite Standardisierung des Abrechnungsverfahrens.

Aus diesem Grund wird zurzeit die Kommunikation zwischen den „Sonstigen Leistungserbringer“ und den Kostentr gern per E-Mail vorangetrieben. Hierbei wird ein hoher Sicherheitsstandard gefordert, da bei der Abrechnung bekanntlich sensible Daten vorhanden sind. Deshalb wird den Teilnehmern am Datenträgeraustausch nach § 300 und § 302 die Verschlüsselung der Daten zwingend auferlegt.

Es liegt bereits seit längerer Zeit ein Gesetzesentwurf zu einem Gesundheitsmodernisierungsgesetz vor. Im Abrechnungsverfahren nach §300 und § 302 ist vorgesehen, dass Leistungserbringer, die aus Gründen, die sie selbst zu verantworten haben, nicht elektronisch und verschlüsselt abrechnen, von den Kostenträgern mit einer pauschalen Rechnungskürzung von bis zu fünf Prozent für die Nacherfassung der Abrechnungsdaten belegt werden können.

Der vorliegende Leitfaden beinhaltet die Grundvoraussetzung für die beiden Abrechnungsverfahren §300 und §302. In beiden Fällen wird die Verschlüsselungssoftware DAKOTA.LE der ITSG zur Erfüllung der vorgeschriebenen Datensicherheit vorausgesetzt.

Zunächst werden der Ablauf der Verschlüsselung und die Systemvoraussetzungen für die Verschlüsselung und den Versand der Dateien beschrieben. Hierbei werden die daraus resultierenden Konsequenzen für die Anwendung des Softwareprogramms erläutert.

Dieser Leitfaden ist auf die Anwendung von mmOrthosoft® ausgerichtet. Sollte darüber hinaus Ihrerseits Klärungsbedarf, insbesondere inhaltlicher, bestehen, wenden Sie sich an Ihre Vertragspartner.

3 Sicherheitskonzept im Gesundheitswesen

Beim dem „alten“ Abrechnungsverfahren in Papierform wurde/wird die Datensicherheit durch das sogar verfassungsrechtlich garantierte Briefgeheimnis garantiert.

Die Einführung des maschinellen Abrechnungsverfahrens ist oftmals mit der Befürchtung verbunden, dass Daten speziell Versichertendaten in die falschen Hände geraten.

Analog zum Briefgeheimnis wird vom Datenschutzbeauftragten des Bundes und der Länder zwingend gefordert, maschinelle Abrechnungsdaten mit personenbezogenen Inhalten zu schützen und somit Manipulationen auf dem Transportweg auszuschließen.

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.

Bei der Abrechnung nach den §300 und §302 hat man sich für ein Asymmetrisches Verschlüsselungsverfahren entschieden

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.

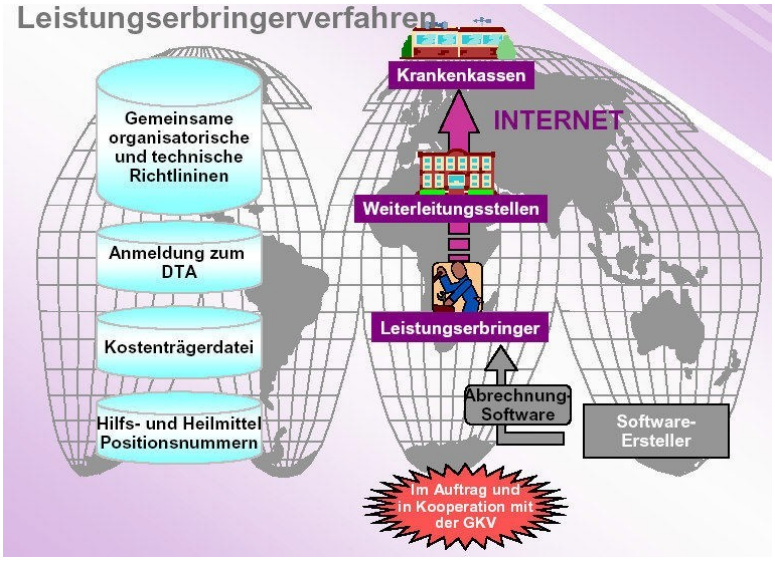
Durch die Verwendung von Verschlüsselung und digitaler Signatur in den Datenaustauschverfahren wird sichergestellt, dass

- 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.



3.1 Funktionsweise der Verschlüsselung

Da beim Datenträgeraustausch zwischen den sonstigen Leistungserbringer und den Kostenträger sensible Daten, d.h. personenbezogene Daten, zusammen mit den Abrechnungsdaten übertragen werden, findet hier die Datenschutzgesetze Anwendung. Die Datenschutzbeauftragten des Bundes und der Länder fordern beim Datenträgeraustausch eine Verschlüsselung dieser Daten.

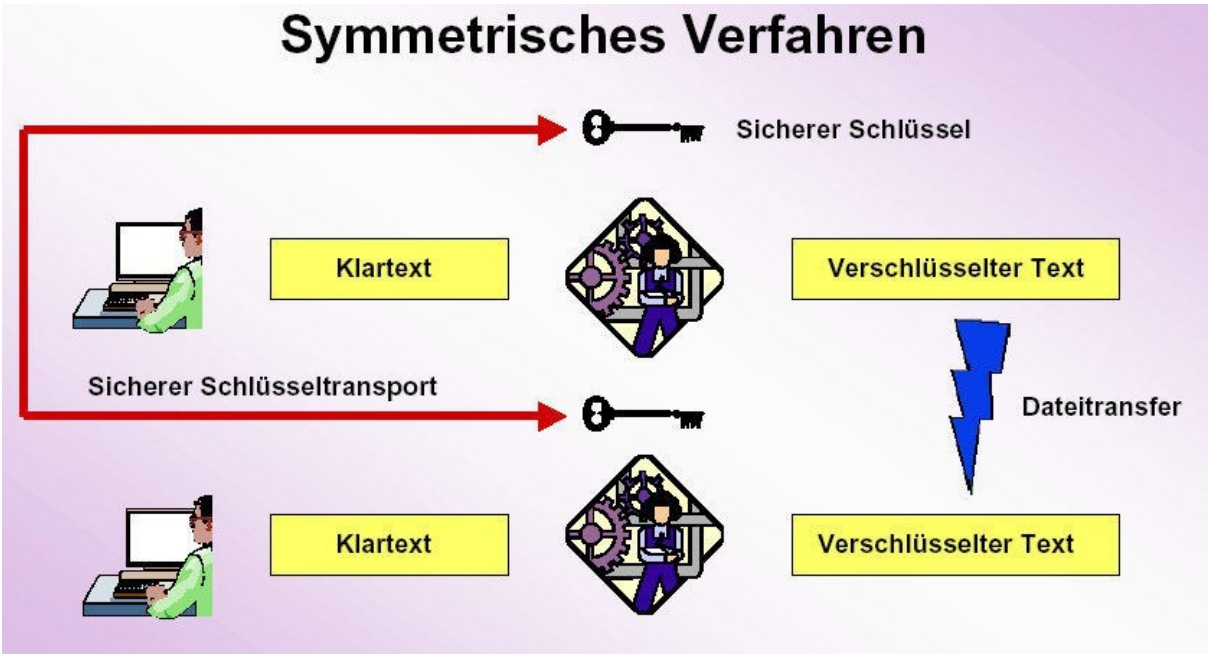
Durch ein mathematisches Verfahren werden die Daten „umgerechnet“ und unkenntlich gemacht. Mit dem entsprechenden Schlüssel kann die Datei wieder entschlüsselt werden.

Es gibt grundsätzlich zwei Verschlüsselungsverfahren:

- Symmetrisches Verfahren,
- Asymmetrisches Verfahren.

3.2 Das symmetrische Verschlüsselungsverfahren

Beim symmetrischen Verfahren wird der Text mit einem sicheren Schlüssel verschlüsselt. Der verschlüsselte Text und der entsprechende Schlüssel werden an den Empfänger gesandt. Der Empfänger kann den verschlüsselten Text mit dem gelieferten Schlüssel entschlüsseln.



Bei jeder weiteren Verschlüsselung muss ein neuer Schlüssel erstellt werden.

Außerdem muss zu jedem Datentransfer ein entsprechender Schlüssel mitgeliefert werden. Aus sicherheitstechnischen Gründen ist eine getrennte Lieferung notwendig.

3.3 Das asymmetrische Verschlüsselungsverfahren

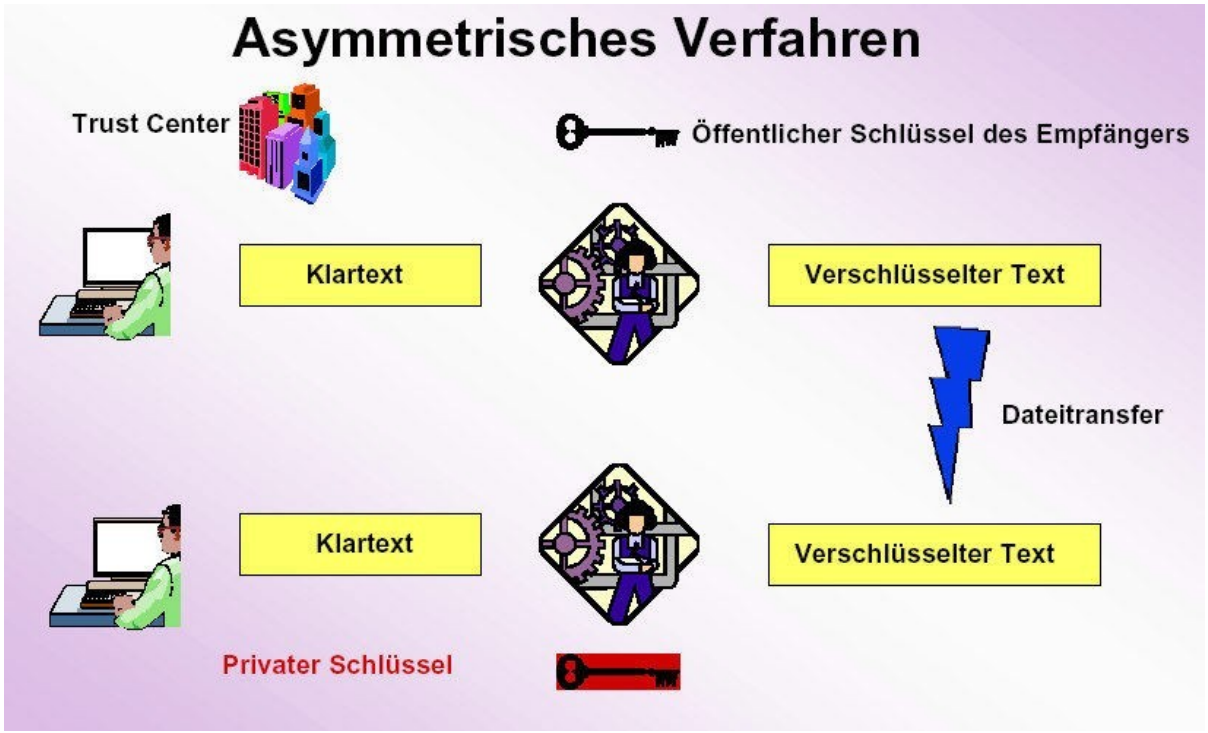
Beim asymmetrischen Verfahren wird der Schlüssel geteilt. Im Prinzip wie früher die in zwei Teile zerrissenen Geldscheine im Wilden Westen. Nur wenn beide Schlüsselhälften (Geldscheine) zusammenpassen kann man die Daten entschlüsseln

Der Geteilte Schlüssel ist dann ein Schlüsselpaar bestehend aus dem

- öffentlichen Schlüssel und
- privaten Schlüssel.

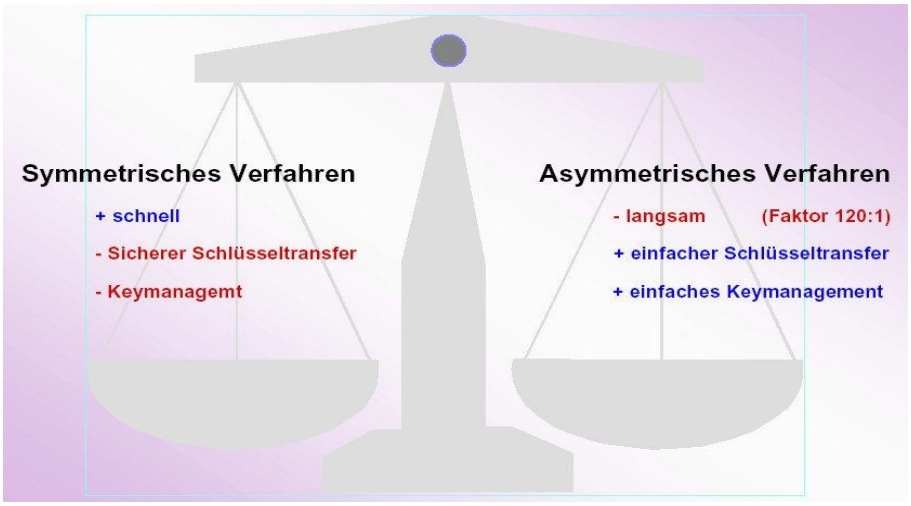
Das TrustCenter verwaltet die öffentlichen Schlüssel und kontrolliert deren Verteilung an berechtigte Empfänger.

Mit dem öffentlichen Schlüssel des Empfängers wird der Text verschlüsselt und versandt. Der passende Schlüssel hierzu ist der private Schlüssel des Empfängers, der nur bei diesem vorliegt. Mit diesem privaten Schlüssel wird der verschlüsselte Text entschlüsselt.



3.4 Gegenüberstellung der Verfahren

Bei der Gegenüberstellung der zwei Verfahren überwiegen trotz des Geschwindigkeitsnachteils das „asymmetrische Verfahren“.



Im Gesundheitswesen hat man sich bei der Verschlüsselung für das asymmetrische Verfahren entschieden.

3.5 Das ITSG Trust Center

Informations
Technische
Servicestelle der
Gesetzlichen Krankenkasse

Da beim Verschlüsselungsverfahren die Teilnehmer auf Authentizität überprüft und die öffentliche Schlüssel sowie der Kostenträger, wie auch der sonstigen Leistungserbringer verwaltet werden müssen, wurde hierzu eine Stelle, das so genannte TrustCenter damit beauftragt.

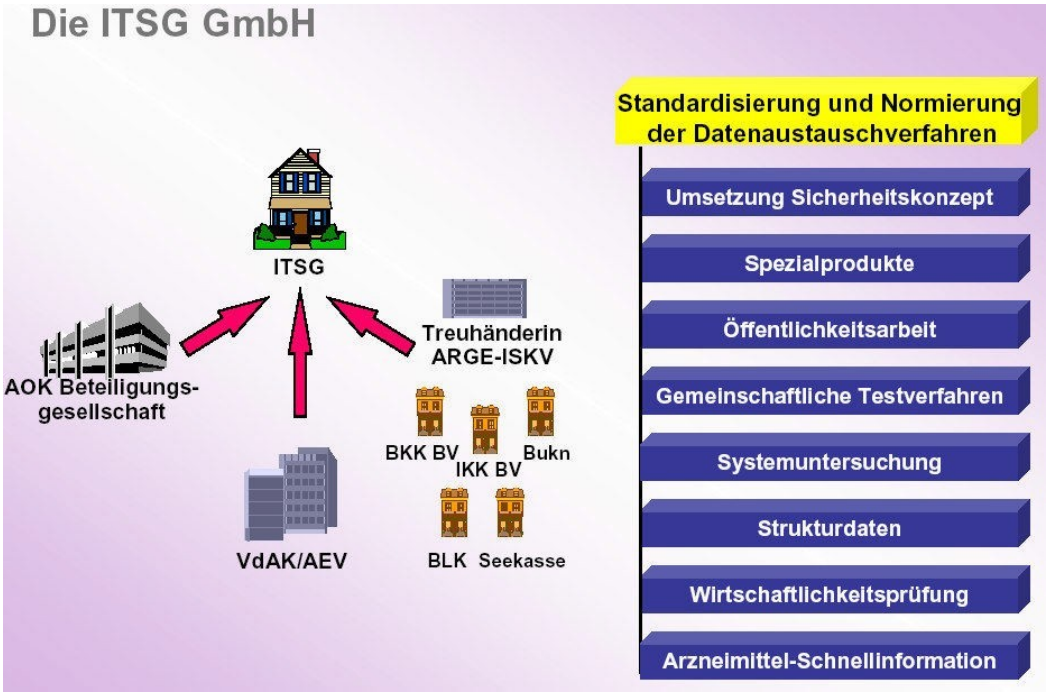
Zur Umsetzung der gesetzlichen Vorgaben Datenträgeraustausch nach § 302 wurde von den Krankenkassen gemeinsame Gesellschaft gegründet, die als Aufgabe die Standardisierung und Normierung des Datenaustauschverfahrens hat.
Dies ist die ITSG in Rodgau.

Des Weiteren hat die ITSG sich folgendes zur Aufgabe gemacht:

- Umsetzung des Sicherheitskonzept
- Spezialprodukte
- Öffentlichkeitsarbeit
- Gemeinschaftliche Testverfahren
- Systemuntersuchungen
- Strukturdaten
- Wirtschaftlichkeitsprüfung
- Arzneimittel-Schnellinformationen

Diese Arbeit wird in Fachgremien der gesetzlichen Krankenkassen ausgearbeitet.
Folgende gesetzlichen Krankenkassen sind an der ITSG in Rodgau Gesellschafter:

- AOK Beteiligungsgesellschaft
- VdAK/AEV
- BKK
- IKK
- Bundesknappschaft
- BLK
- Seekasse



Die ITSG als Dachverband der gesetzlichen Krankenversicherung hat einer externen Firma die Aufgabe des TrustCenters anvertraut. Das TrustCenter für das Gesundheitswesen ist das TrustCenter CCI in Meppen.

Diese Firma hat den Auftrag, den Aufbau und Betrieb eines TrustCenters für den Datenaustausch im Gesundheitswesen umzusetzen. Ziel ist die gesicherte Kommunikation zwischen den Leistungserbringern und den Annahmestellen der Kostenträger.

3.6 Die Verschlüsselungssoftware DAKOTA.LE

DAtenaustausch und
KOmmunikation auf Basis
Technischer
Anlagen für die sonstigen
LEistungserbringer

Zum Zweck der Vorgabenerfüllung wurde von der ITSG die Verschlüsselungssoftware DAKOTA.LE entwickelt. Es ist nur möglich mit den Kostenträgern direkt abzurechnen wenn man diese Verschlüsselungssoftware einsetzt. Es gibt KEINE Alternative zu DAKOTA.LE

ANMERKUNG:
Wir von mmOrthosoft® haben in diesem Fall keinen Einfluss auf Kostenstruktur und Leistungsumfang dieser Fremdsoftware. Die Software muss wie angeboten vergütet und eingesetzt werden.

Das ITSG TrustCenter stellt die Identität des Teilnehmers fest und lässt ihn zum Datenaustauschverfahren zu. D.h. der Abrechnungsschlüssel wird personenbezogen ausgestellt. Diese Authentizität wird anhand der beim Antrag beigefügten Unterlagen überprüft. Folgende Unterlagen müssen zur Antragstellung gesandt werden:

- Ausgefüllter und unterschriebener Antrag (2 Seiten)
- Kopie des IK-Nummerbescheides der Vergabestelle
- Kopie eines persönlichen Dokumentes, das den Ansprechpartner ausweist
- Elektronischer Zertifizierungsantrag

Die Überprüfung der Unterlagen erfolgt auf Vollständigkeit und Unterschrift, die des öffentlichen Schlüssels auf Eindeutigkeit.
Nach der Überprüfung wird der öffentliche Schlüssel zertifiziert und in das Schlüsselverzeichnis aufgenommen.
Das TrustCenter verteilt an alle teilnehmenden Kostenträger den öffentlichen Schlüssel des sonstigen Leistungserbringers und sendet dem Antragsteller die öffentlichen Schlüssel der Kostenträger zu. Außerdem erhält der Antragsteller eine Zertifizierungsantwort.

Das TrustCenter führt auch eine Sperrliste, wenn Schlüssel abgelaufen oder gesperrt werden müssen.

3.7 Antragsverfahren

Der Ablauf des Antragverfahrens ist wie folgt:

Im ersten Schritt wird nach der Installation der DAKOTA Software das Antragsformular am Bildschirm ausgefüllt. Danach wird per Zufallsgenerator der Schlüssel erstellt. Das Antragsformular und der per Zufallsgenerator erzeugte Schlüssel werden online an das Trust Center übermittelt.

Im zweiten Schritt muss das erstellte Antragsformular dann lokal auf Papier nochmal ausgedruckt, unterschrieben und zusammen mit einem Identifikationsnachweis des

Antragstellers und einer Kopie des IK Nummer Vergabebescheides an die angegebene Faxnummer der ITSG nachgesendet werden.

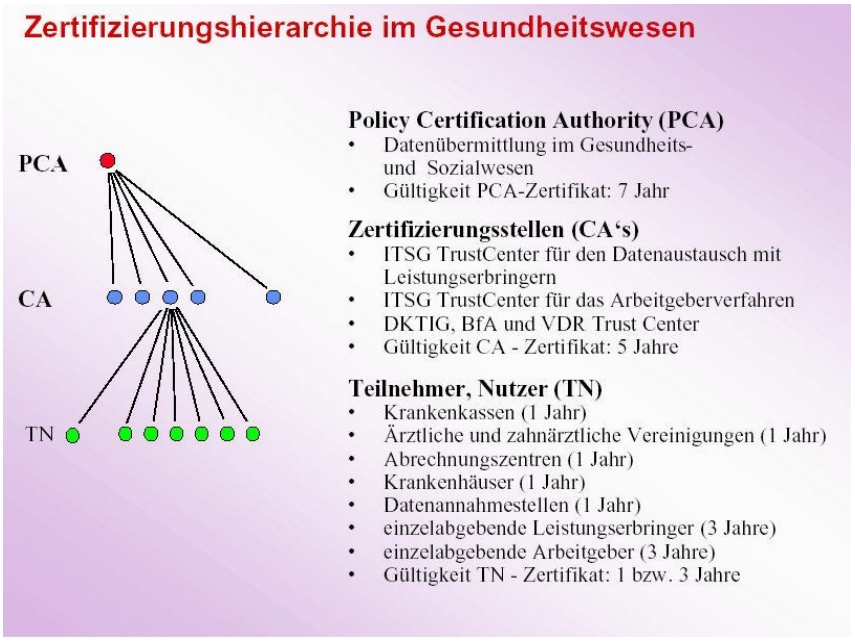
HINWEIS:
Nur wenn beides, also der elektronische Antrag und der unterschriebene Papierantrag bei der ITSG vorliegen wird ein Zertifikat innerhalb von maximal 8 Tagen, ausgestellt.

3.8 Laufzeit der Schlüssel Zertifikate

Wie bereits beschrieben, wird der Klartext anhand der Verschlüsselung in einem aufwändigen mathematischen Verfahren unkenntlich gemacht. Es gibt Personen, die versuchen, jedes Sicherheitskonzept zu knacken. Das bedeutet, die absolute, dauerhafte Sicherheit gibt es nicht. Es ist nur eine Frage der Zeit, bis die Verschlüsselung geknackt werden kann.

Bei dem asymmetrischen System der Verschlüsselung benötigt man zum hacken des Schlüssels bei modernster Technik ca. 10 Jahre. Aus diesem Grund sind die Zertifikate und somit die Schlüssel zeitlich begrenzt.

Bei den Laufzeiten hat man hierbei eine Zertifizierungshierachie für das Gesundheitswesen aufgebaut. So müssen die Zertifizierungsstellen selbst alle fünf Jahre einen neuen Schlüssel erstellen, die Leistungserbringer alle drei Jahre und die Datenannahmestellen der Kostenträger sogar jedes Jahr einen neuen Schlüssel zertifizieren lassen.



HINWEIS:
Die Laufzeit der Schlüssel für Sonstige Leistungserbringer beträgt bis Dato:

3 Jahre

Vorschlag:
Setzen Sie sich das Ablaufdatum Ihres Schlüssels nach dem Einlesen auf Wiedervorlage ca. 2-3 Wochen vor dem eigentlichen Ablauf.

4 Voraussetzungen

Für die Einrichtung und Installation der DAKOTA Verschlüsselung-Software sollten Sie vorab folgende Voraussetzungen schaffen:

[ ] Windows Administratordaten und Passwort bereithalten
Wird nur einmalig für die Installation der DAKOTA Software benötigt.
Fragen Sie Ihren Hardwarepartner

[ ] E-Mail Konto Zugangsdaten und Passwörter bereithalten

Die Abwicklung der elektronischen Abrechnung läuft über das E-Mail Verfahren. Dafür ist eine gültige E-Mail Adresse notwendig. Sollten Sie nicht über ein eigenes E-Mail Konto z.B. über Ihre Homepage verfügen, können Sie jederzeit, auch nur für diesen Zweck, ein sogenanntes „freemail“ Konto bei einem öffentlichen Anbieter wie:

gmx.de web.de google.de t-online.de u.v.m.

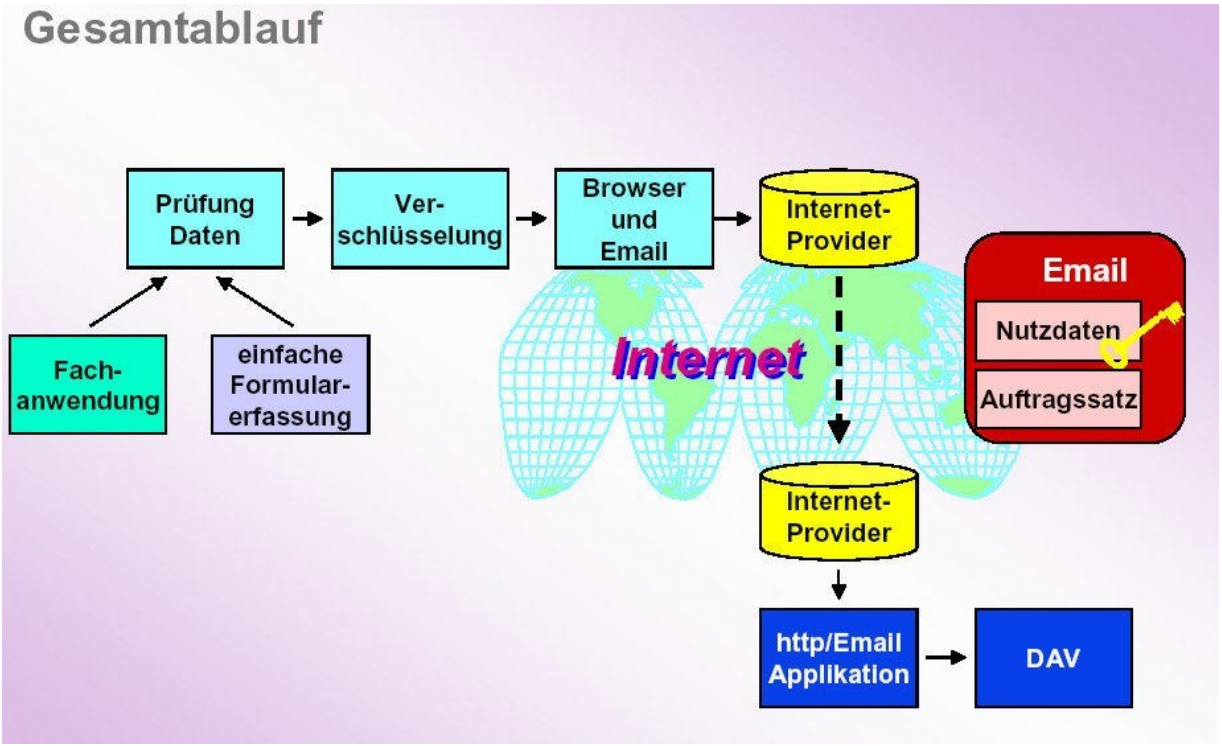
4.1 E-Mail Verfahren

Der Gesetzgeber verankerte im Gesundheitsstrukturgesetz von 1992, dass für die Abrechnung zwischen den Leistungserbringer und Kostenträgern Kosten sparende und moderne Technologien genutzt werden müssen.

Die ITSG als Dachverband der Kostenträger versucht dies auch konsequent umzusetzen. Sie stellt die Anforderungen für die Kostenträgerorganisationen und Softwareanbieter und schafft damit die Grundlagen für den Datenträgeraustausch.

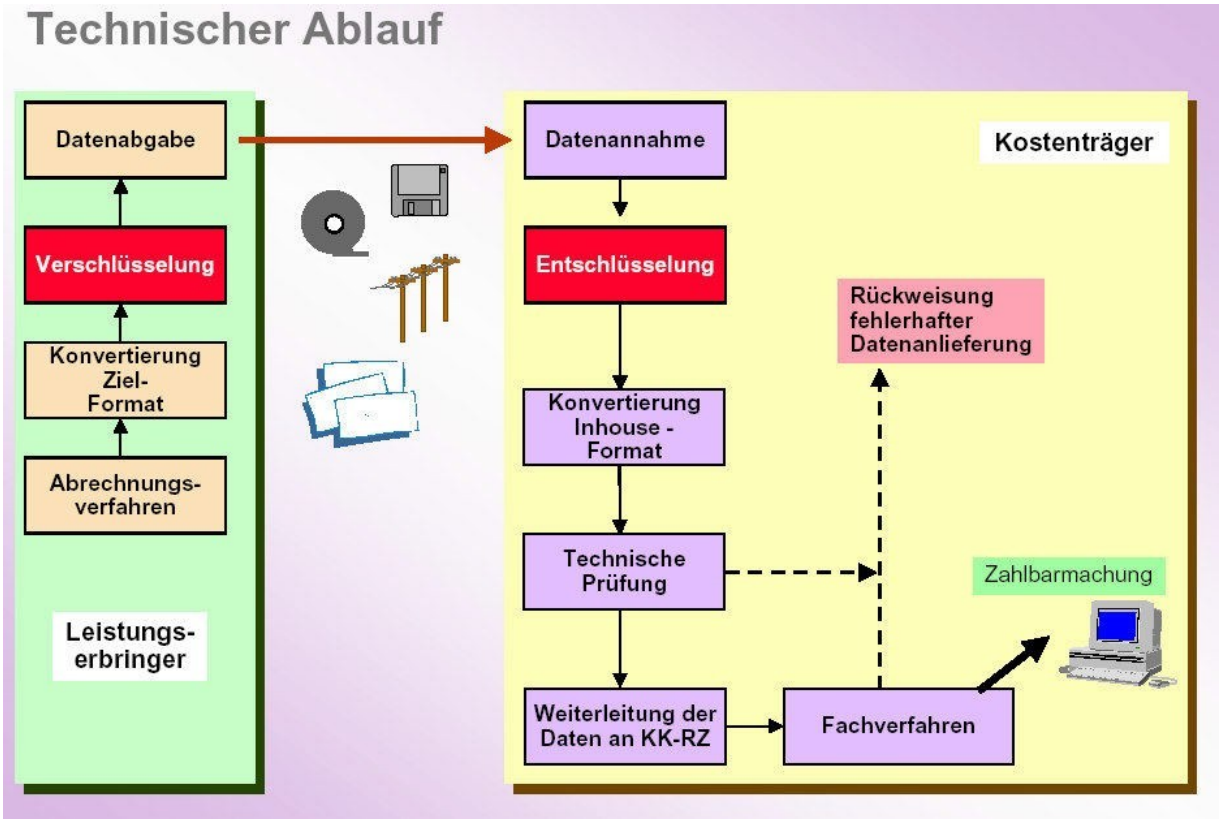
Eine Voraussetzung für den Datenaustausch nach § 302 ist die Verschlüsselung und Versendung der Dateien per E-Mail.

Im Prozess des Datenträgeraustausches der Abrechnungsdaten werden die Abrechnungsdaten wie bisher erfasst. Schon während der Erfassung der Daten werden prüfbare Datenfelder überprüft.
Bei der Dateierstellung der Abrechnungsdaten werden die Daten nochmals auf Vollständigkeit der Mussfelder überprüft. Anschließend werden die Daten mit dem Verschlüsselungsmodul verschlüsselt und per E-Mail an einen Internetprovider übergeben.
Die E-Mail besteht aus der verschlüsselten Nutzdatei und dem Auftragssatz.
Über den Internetprovider empfängt die Datenannahmestelle des Kostenträgers die E-Mail und reicht dies an die entsprechende Stelle weiter.



Die E-Mail bestehend aus Auftragsdatei und verschlüsselten Daten und wird über das Internet an die Annahmestelle des Kostenträgers gesandt.

Betrachten wir noch einmal den technischen Ablauf:

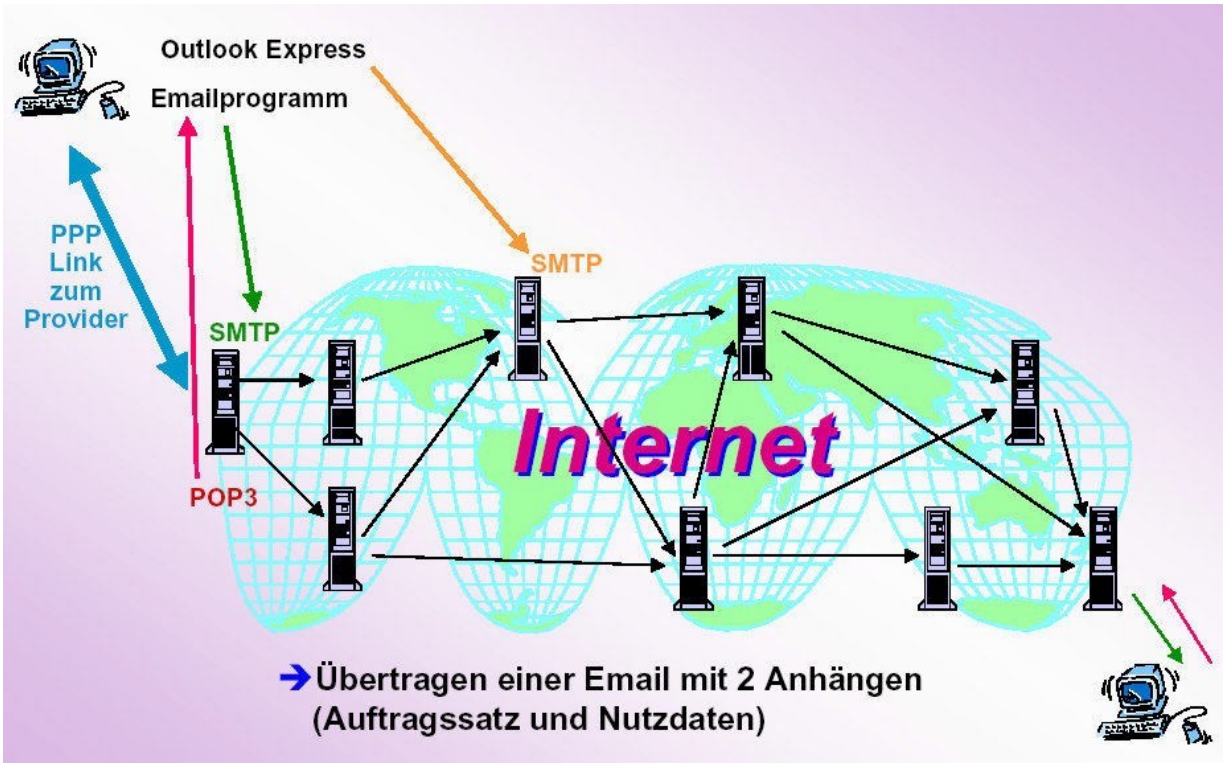


Die Daten des Leistungserbringers werden verschlüsselt und versendet.
Nach der Datenannahme werden die Daten von der Annahmestelle des Kostenträgers entschlüsselt und auf das Format der jeweiligen Anwendung konvertiert. Danach findet die technische Prüfung statt, z.B. ob die Daten gelesen werden können, die Feldlänge korrekt ist etc.

Sollten Fehler vorliegen, wird der Absender darüber per E-Mail informiert. Andernfalls werden die Daten an die entsprechenden Krankenkassenrechenzentren und Fachabteilungen weitergeleitet. Sollten hier Unstimmigkeiten vorliegen, wird der Absender ebenfalls per E-Mail darüber informiert.

Für die Übertragung der E-Mail wird ein Internetzugang vorausgesetzt. Die Versendung erfolgt mit Outlook Express®. Sollten andere E-Mail-Programme eingesetzt werden, müssen diese einen direkten Zugriff auf den SMTP-Server haben.
Aufgrund der daraus resultierenden Varianten an Problemen können wir nur Outlook Express® unterstützen.

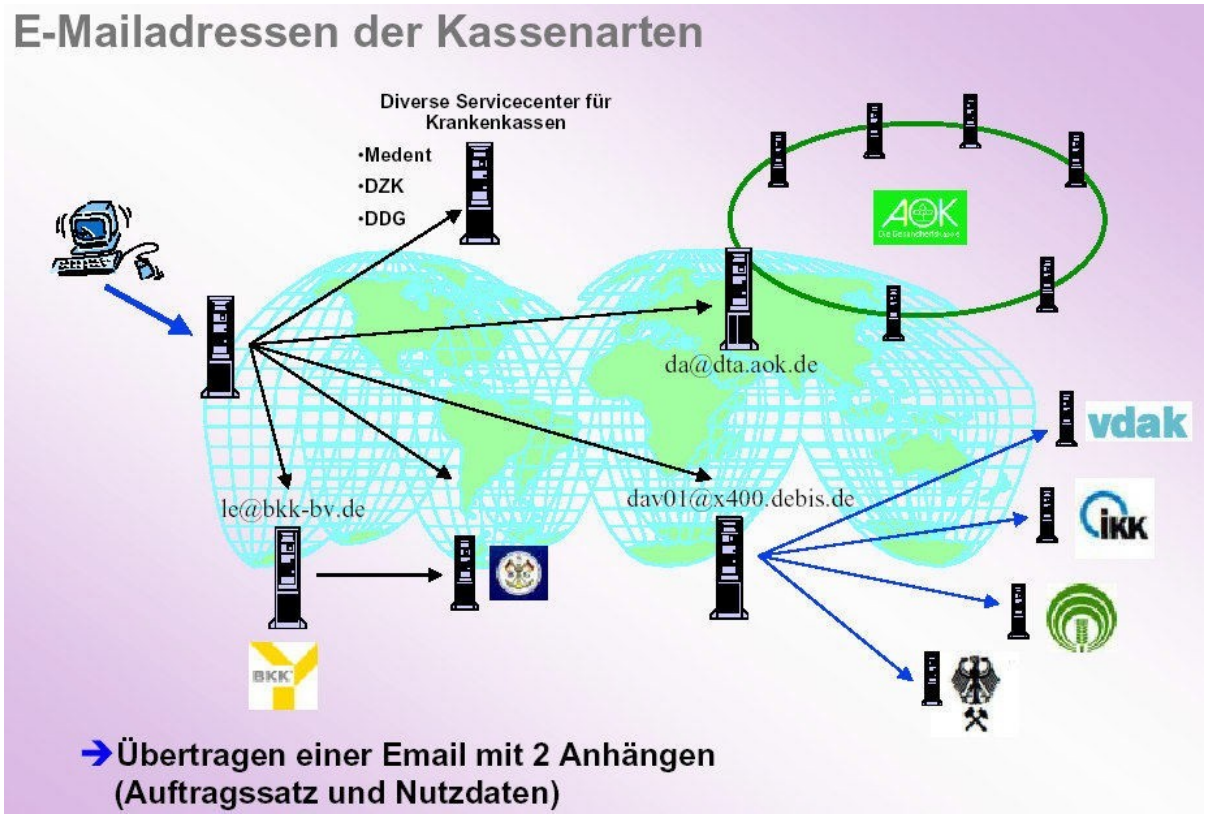
Eine weitere Variante ist die Versendung direkt aus dem § 302-Modul. Voraussetzung ist hier, dass bereits eine Internetverbindung besteht, da sich das Modul nicht selbst einwählen kann.



Aufbau eines E-Mail

FROM	***Absender***	BN- oder IK-Nummer des Absenders	zwingend
	Absender E-Mailadresse	E-Mailadresse des Absenders	zwingend
TO	***Empfänger***	Name der Annahmestelle	zwingend
	Empfänger E-Mailadresse	E-Mailadresse der Annahmestelle	zwingend
SUBJECT	***Betreff***	IK-Nummer des Absenders	zwingend
MESSAGE BODY	***Nachrichteninhalt***	Dateiname Auftragssatz, Länge in Byte, Datum und Uhrzeit der Erstellung <CR LF> Dateiname Nutzdaten, Länge in Byte, Datum und Uhrzeit der Erstellung <CR LF> Absenderinformationen	optional
ATTATCHMENT	***Anhang 1***	Datei mit dem Auftragssatz	zwingend
	Anhang 2	Datei mit den Nutzdaten	zwingend

Die E-Mail-Adressen der Annahmestellen sind im Verschlüsselungsmodul hinterlegt. Das bedeutet, mit der Versendung der verschlüsselten Daten wird die entsprechende E-Mail-Adresse automatisch angewählt.



4.2 E-Mail Provider

Die Übertragung der E-Mails erfolgt über einen E-Mail Provider.
Als Provider können nur diejenigen benutzt werden welche mit einem SMPT-Server und POP3-Server arbeiten.

Provider mit einer geschlossenen E-Mail-Anwendung können nicht benutzt werden. Dies ist z.B. bei AOL der Fall.

Sollten Sie keine Mailadresse besitzen oder diese Mails ganz getrennt von Ihren Geschäftsmails abwickeln wollen empfehlen wir einfach eine Free Mail Adresse anzulegen. z.B. unter:

www.gmx.de
www.google.de
…

4.3 Einrichten eines separaten E-Mail Kontos

Viele Benutzer richten sich nur für den Datenaustausch ein separates E-Mail Konto bei einem öffentlichen Provider wie GMX.DE, GOOGLE.COM, WEB.DE usw. ein.

Die Zugangsdaten für dieses E-Mail Konto können dann ganz einfach in der DAKOTA Software für den Datenaustausch eingetragen und benutzt werden

Rufen Sie dazu einfach die Homepage eines Providers auf. In der Regel gibt es einen Link wie z.B. „Kostenlos anmelden“. Folgen Sie einfach diesem Link und vergeben dabei eine E-Mailadresse und ein Kennwort.

Diese Mailadresse und das vergebene Kennwort kann dan zu einem späteren Zeitpunkt bei der Installation der DAKOTA Software verwendet werden.

5 DAKOTA aus Mailbox downloaden

Das Verschlüsselungsmodul ist ein Fremdprodukt und wird in mmOrthosoft® integriert. Dies hat für den Anwender den Vorteil, dass er sich nicht um Datenkopieren und manueller Verschlüsselung kümmern muss. Dies ist gerade für den nicht versierten Anwender von großer Bedeutung. Außerdem können die Vorgänge direkt unserem Produkt protokolliert werden.

Das Verschlüsselungsmodul DAKOTA wird in der Mailbox zur Verfügung gestellt. Zum Downloaden wird ein entsprechendes Passwort benötigt, das sich täglich ändert. Aus diesem Grund muss hierzu das Tagespasswort beantragt werden.

Unter:

Extras - Systemeinstellungen - §302/§300 - Setup Verschlüsselungssystem

gibt es die Möglichkeit, den Passwortantrag auszudrucken oder direkt zu faxen.

Sie erhalten dann umgehend das Passwort, das Ihnen zum Downloaden des Verschlüsselungsmoduls und zum Einrichten dient. Diese Passworte sind nur tageweise gültig. Die Mailbox wird gestartet in mmOrthosoft® unter:

EXTRAS > Mailbox

Nach dem Aufruf finden Sie die DAKOTA Verschlüsselungssoftware unter:

- **302-Verschlüsselung.**

Hier ist das Verschlüsselungsmodul hinterlegt und kann nach Eingabe des Passwortes heruntergeladen werden.

Markieren Sie die Software durch setzten eines Hakens bei:

(x) mmcrypt…(Immer die höchste Version auswählen)

Und klicken anschließend auf

<DOWNLOAD>

Hinweis:
Das laden kann je nach Geschwindigkeit einige Zeit in Anspruch nehmen

6 DAKOTA Software Konfiguration

6.1 DAKOTA SETUP starten

Nach dem Downloaden gehen Sie an die Arbeitsstation, die für die Verschlüsselung bestimmt ist, Melden sich wie folgt an:

-Im Windows als Administrator (Volle Rechte auf dem Windows PC)
-Im mmOrthosoft mit „Master“ (Volle Rechte in mmOrthosoft)

In mmOrthosoft® rufen Sie das DAKOTA SETUP auf unter:

Extras >Systemeinstellungen>Firma >DTA §302/§300> DAKOTA.LE>
Setup Verschlüsselungssystem

Zum Einrichten wird das Tagespasswort benötigt, das Sie mit entsprechendem Formular bereits beantragt und erhalten haben.

Sollte die Einrichtung an einem anderen Tag als der Download erfolgen, wird ein neues Tagespasswort benötigt. Dieses können Sie mit der Programmfunktion Antragsformular beantragen.

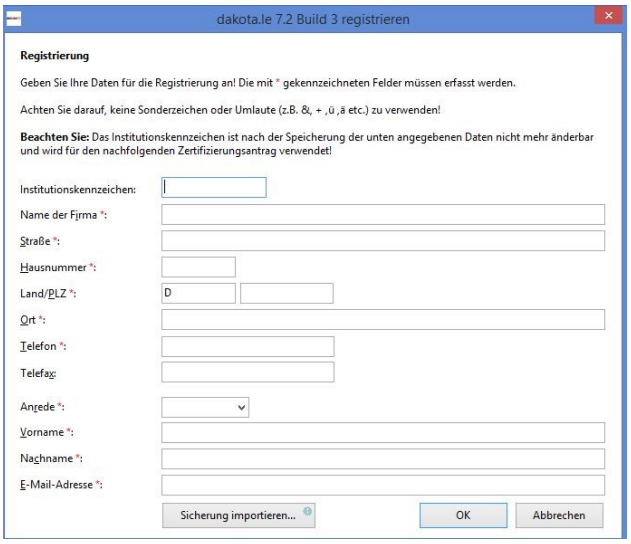
Nach Eintragung des Tagespasswortes beginnt die Entpackung und Installation von DAKOTA

HINWEIS:

Die Installation kann je nach Version und Computerausstattung mehrere Minuten Zeit in Anspruch nehmen wo auf dem Bildschirm nichts passiert. Bitte haben Sie etwas Geduld.

6.2 Registrierung

Ist das Setup durchgelaufen werden sie direkt aufgefordert sich zu registrieren
Füllen Sie die Daten wie am Bildschirm gefordert korrekt aus.

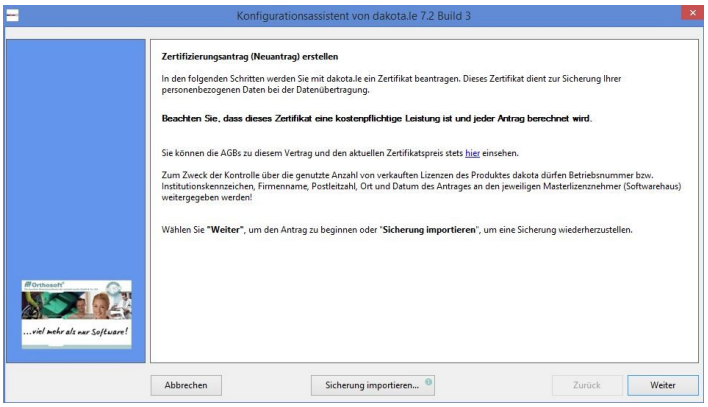


6.2.1 Sicherung importieren

Sollte eine Sicherung einer aktuellen DAKOTA Version vorhanden sein kann diese importiert werden über:
<Sicherung importieren>

6.3 Dakota Assistent

Nachdem Sie sich registriert haben wird der DAKOTA ASSISTENT gestartet der Sie durch die Installation führt. Für einen NEUEN Zertifizierungsantrag klicken Sie auf
<WEITER>

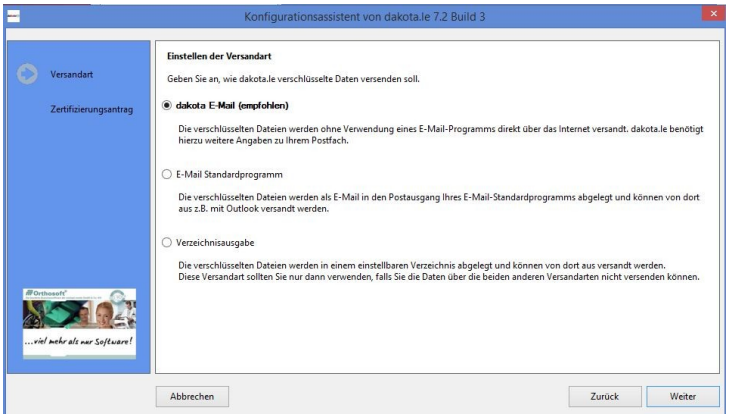


6.3.1 Sicherung importieren

Sollte eine Sicherung einer aktuellen DAKOTA Version vorhanden sein kann auch an dieser Stelle diese importiert werden über:
<Sicherung importieren>

6.4 Versandart

In der ersten Maske wird das Übertragungsverfahren festgelegt.



[x] dakota E-Mail (Empfohlen)

Direktübertragungsverfahren. Dieses Verfahren wird empfohlen und auch in den meisten Fällen benutzt. Wählen Sie im nächsten Schritt Ihren Mailprovider aus und geben die Zugangsdaten direkt ein. Bei dieser Einstellung wird Outlook zum Versenden nicht benötigt, da DAKOTA die Daten sozusagen direkt bei Ihrem Provider ablegt. Die genauen Zugangsdaten erhalten Sie von

Ihrem Provider direkt. Nach Eingabe Zugangsdaten wird eine Testverbindung aufgebaut um sicher zu stellen, dass das Übertragen der Daten gewährleistet ist.

[ ] E-Mail Standardprogramm

Wollen Sie die Daten nicht direkt versenden sondern über ein „lokales“ MAIL Programm versenden, wählen Sie hier Ihr E-Mail Standardprogramm, meist Outlook oder Outlook Express. Bei diesem Verfahren müssen die Zugangsdaten in dem jeweiligen Mailprogramm hinterlegt werden, damit dieses Ihre E-Mails abrufen und versenden kann.

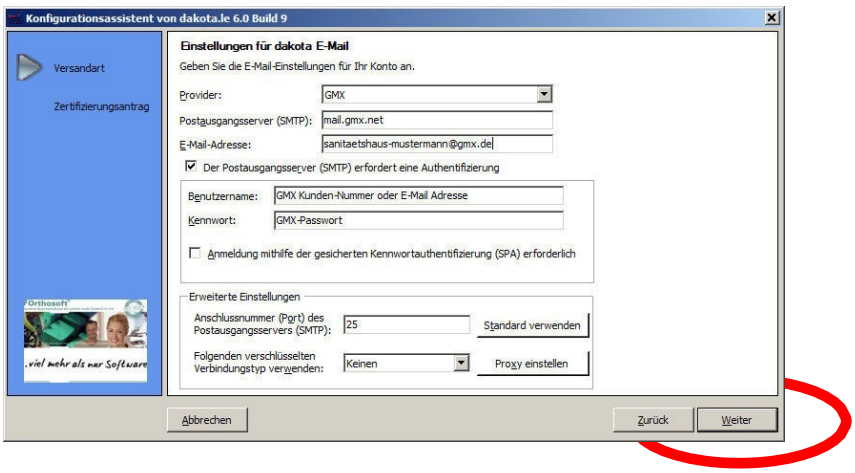
[ ] Verzeichnisausgabe

Diese Variante gibt die Daten einfach in ein Verzeichnis aus.
Sie ist für die Benutzung von mmOrthosoft® irrelevant und wird nie verwendet.

Mit WEITER kommen Sie zum nächsten Schritt

6.5 E-Mail Provider Zugangsdaten hinterlegen

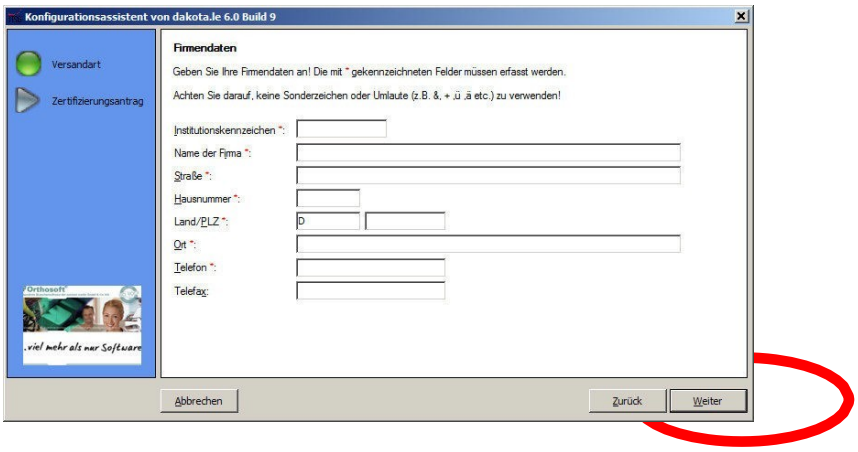
In der nächsten Maske werden die Zugangsdaten zu Ihrem E-Mail Provider hinterlegt. Wählen Sie bei PROVIDER einen vordefinierten Zugang aus werden alle Grundeinstellungen vorbelegt und Sie müssen nur noch Ihre E-Mail Adresse und das entsprechende Passwort hinterlegen.



Nach Eingabe der Zugangsdaten wird ein Test durchgeführt ob die Daten gültig sind.

6.6 Zertifizierungsantrag ausfüllen

Für den Zertifizierungsantrag geben Sie hier Ihre IK Nummer und Daten wie gefordert ein.



Mit WEITER kommen Sie zum nächsten Schritt

6.7 Ansprechpartner

Da der Schlüssel personenbezogen ausgestellt wird ist die Auswahl des Ansprechpartners von einiger Bedeutung. Es sollte auf alle Fälle eine integere Person sein die langfristig im Unternehmen beschäftig ist. Von diesem Ansprechpartner muss auch eine Kopie des Personalausweises oder dem Führerschein als Anlage mit dem Antrag mitgeschickt werden.

Mit **WEITER** kommen Sie zum nächsten Schritt

Es werden noch Passwörter und Zugangscodes abgefragt welche sehr kurz und allgemeingültig gehalten werden können.

Mit **WEITER** kommen Sie zum nächsten Schritt

Es erscheint eine Zusammenfassung der eingegebenen Daten zum Überprüfen und ausdrucken.
Dieser Ausdruck ist NUR für Ihre Ablage!
Das ist noch NICHT der Zertifizierungsantrag!

6.8 Antrag elektronisch versenden

An dieser Stelle wird per Zufallsgenerator ein Schlüssel generiert.
Nach dem Erzeugen des Schlüssels wird dieser automatisch zusammen mit dem Zertifizierungsantrag mit allen wesentlichen Angaben an das Trust Center per Mail bzw. wenn eine Internetverbindung besteht direkt per FTP versendet.
Erst wenn beide Anträge, also der elektronisch versendete und der Papierantrag mit Unterschrift bei der ITSG vorliegen wird ein Zertifikat ausgestellt.

Mit WEITER kommen Sie zum nächsten Schritt

6.9 Antrag ausdrucken unterschreiben und faxen

Nun werden Sie aufgefordert, den Antrag in Papierform auszudrucken zum Unterschreiben. Füllen Sie die Felder zur Branchensoftware manuell aus.

Lassen Sie den Antrag vom Antragsteller unterschreiben und faxen ihn komplett zusammen mit den Anlagen:

- Kopie Reisepass oder Führerschein des Ansprechpartners und
- Kopie IK Nummer Vergabebescheides

An die auf dem Antrag genannte Faxnummer.

Erst wenn die Datei per E-Mail und der schriftliche Antrag zusammen dort sind, wird der Vorgang bearbeitet. Die Bearbeitung dauert lt. ITSG maximal 8 Werktage.

ITSG Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH

ITSG

Zertifizierungsantrag

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

IK*[1] 1 2 3 4 5 6 7 8 9 oder Betriebsnummer*[2]

HashCode: 0D 1B 07 52 5D 0E 2F 15 49 89 BF 8D 99 8A E4 2E

1. Antragsteller

Sanit ae tshaus M ue ller — Name des Antragstellers* (Firma / Institution)

06227-838300 — Telefon-Nr.

Frank Menger — verantwortlicher Ansprechpartner*

06227-838399 — Telefax-Nr.

Daimlerstrasse 42 — Straße

hotline@mmorthosoft.de — E-Mail-Adresse

69190 Walldorf — PLZ Ort

[X] 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 (\, +, &, Semikolon, Unterstrich, Komma, \, Anführungszeichen, § etc.). Das Trust Center 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 des **Personalausweises**, **Reisepasses** oder **Führerscheins** des Ansprechpartners beizufügen. Im Leistungserbringerverfahren 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.

3. Angaben zur eingesetzten Software (freiwillige Angabe)

Mit welchem Softwarehaus arbeiten Sie zusammen? michael martin GmbH+Co.KG

Welche Fachanwendung setzen Sie ein? mmOrthosoft©

Lizenznummer: 00004711

4. Schlüsselgenerierung

Meine/Unsere Software zur Schlüsselgenerierung hat eine Datei erstellt, in der alle wesentlichen Angaben des vom Trust Center später zu erstellenden Zertifikates bereits enthalten sind (Format: 12312312.crq). Die Datei wurde/wird übermittelt

[X] per E-Mail, (ITSG-CRQ@ATOSORIGIN.COM)

1 Das Institutionskennzeichen (IK-Nummer) erhalten Sie von der SVI Arbeitsgemeinschaft Institutionskennzeichen auf Anfrage erteilt.

2 Die Betriebsnummer wird von Ihrer zuständigen Bundesagentur für Arbeit erteilt.

ITSG Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH

ITSG

IK: 123456789

5. Kundenkennwort

Um persönliche Auskünfte am Telefon zu erhalten, muss der Kunde sein Kennwort nennen. Wählen Sie als Kundenkennwort ein beliebiges Wort bis zu 12 Zeichen.

Das Kundenkennwort ist: _____

6. Sperrung

Bitte ankreuzen, wenn die telefonische Sperrung des Zertifikates wegen möglicher Eilbedürftigkeit auch durch Personen erfolgen soll, die das Kundenkennwort nicht kennen.

[ ] Eine Sperrung des Zertifikates per Telefon soll auch ohne Angabe eines Kundenkennwortes möglich sein.

7. Rechnungsanschrift

Nur auszufüllen falls von o.g. Anschrift abweichend. Der Rechnungsempfänger ist zum Empfang von an die Kunden gerichteten Mitteilungen bevollmächtigt.

Name/Firma _____

Straße oder Postfach _____

PLZ _____ Ort _____

8. Zahlungsweise

Das Entgelt für die Zertifizierung entnehmen Sie bitte der aktuellen Preisliste des ITSG Trust Centers (www.itsg.de). Sofern nicht gesondert ausgewiesen, wird jeder Zertifizierungsvorgang in Rechnung gestellt.

9. Bemerkungen / Besonderheiten

_____

_____

_____

_____

10. Unterschrift des verantwortlichen Ansprechpartners

Ich bestätige diesen Auftrag gemäß den ausgehändigten allgemeinen Geschäftsbedingungen (AGB) des ITSG Trust Centers, Stand 01.09.2005. Ich bestätige insbesondere, dass ich

- die Notwendigkeit der Veröffentlichung des Zertifikates in elektronischen Verzeichnissen anerkenne,
- die Verantwortung für den Schutz meines privaten Schlüssels vor Missbrauch durch Unbefugte übernehme,
- Passwörter und PINs zum Schutz des privaten Schlüssels geheimhalte,
- bei Preisgabe oder Verdacht der Preisgabe von Passwort oder PIN diese unverzüglich ändern werde und
- bei Kompromittierung meines privaten Schlüssels unverzüglich die Sperrung des Zertifikates durch das ITSG Trust Center veranlassen werde.

22.05.2007 13:46:46 — Datum

_____ — Unterschrift

Bitte senden Sie den 2-seitigen Zertifizierungsantrag und die Kopien für die Identitätsfeststellung per Post oder Fax an:

-> per Post an ITSG Trust Center, Postfach 12 30, D-49702 Meppen

-> per Fax an ITSG Trust Center, +49 5931 848 840

Anlagen:

- Kopie(n) für die Identitätsfeststellung
- Unterschriebener Ausdruck des öffentlichen Schlüssels
- Ggf. Vollmacht des Antragstellers für den verantwortlichen Ansprechpartner

ACHTUNG: Bitte füllen Sie noch MANUELL folgende Felder des ausgedruckten Antrages:

Mit welchem Softwarehaus arbeiten Sie zusammen?
Michael Martin GmbH & Co.KG

Welche Fachanwendungen setzen Sie ein?
mmOrthosoft®

6.10 Sichern des Schlüssels

Führen Sie wie gefordert eine Sicherung des Antrags und des Schlüssels durch.
Am Besten auf dem Netzlaufwerk wo abends auch eine Datensicherung durchgeführt wird.
Wir empfehlen unterhalb des \ORTHO Verzeichnisses. Z.B.:
o:\ortho\dakotabackup

Falls zwischen Antragerstellung und einlesen des Zertifikats Probleme mit der Hardware auftauchen sollten, ist es sinnvoll, den Schlüssel unabhängig zu sichern.

Folgen Sie den restlichen Anweisungen und verlassen danach das Programm

7 Einlesen des zertifizierten Schlüssels

Wenn der Antrag erfolgreich bearbeitet wurde; erhalten Sie von der ITSG innerhalb weniger Tage (maximal 7 Tage) eine Antwortmail mit zwei Dateianhängen.

ACHTUNG: bitte versuchen Sie NICHT diese Dateianhänge zu öffnen!

Laden Sie die Dateianhänge dieser Mail in ein beliebiges Verzeichnis herunter.

Zum Einlesen des Schlüssels starten Sie Dakota unter:

EXTRAS >SYSTEMEINSTELLUNGEN >FIRMA >DTA§302/300>Dakota.le>
> Verschlüsselungsassistent

Es meldet sich der Konfigurationsassistent an der Stelle an der Sie ihn das letzte Mal verlassen haben.

Sie haben nun zwei Möglichkeiten das Zertifikat einzulesen

- Direkt über das Internet über die Antragsnummer
- Einlesen der E-Mail Anhänge

Die schnellste Variante ist die Eingabe der Auftragsnummer und der Klick auf den Button **ABHOHOLEN**. So wird der Schlüssel direkt über das Internet eingelesen.

Die Zweite Variante ist Einlesen der E-Mail Anhänge

Klicken Sie auf DURCHSUCHEN und gehen auf das Verzeichnis indem Sie die E-Mail Anhänge gespeichert haben und klicken auf EINLESEN

ACHTUNG: Mit der Antwort-E-Mail erhalten Sie auch eine Auftragsnummer über die Sie die Zertifikate direkt über das Internet abholen und einlesen können.

Mit **OK** und **WEITER** kommen Sie zum nächsten Schritt

Als zweites wird der Annahme-Key eingelesen. Klicken Sie nochmals auf DURCHSUCHEN und gehen auf das Verzeichnis; in das Sie die E-Mail Anhänge gespeichert haben.

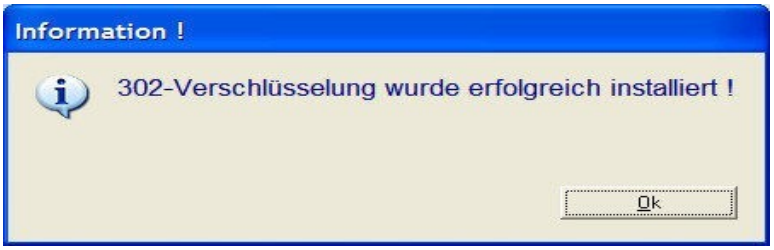
W hlen Sie die Datei mit der Endung …..KEY aus

Mit **OK** und **WEITER** kommen Sie zum nächsten Schritt

HINWEIS:
SICHERN Sie den Schlüssel auf ein Laufwerk, was auch in der Datensicherung berücksichtigt wird!

Die Verschlüsselungssoftware ist nun Schlüsselfertig und kann eingesetzt werden

Mit Beenden können Sie das Programm verlassen.



8 DAKOTA Programm Assistent

Ist ein neuer Schlüssel zu beantragen, ein neuer Annahme-Key einzulesen, die Stammdaten der Abrechnungsstellen einzulesen oder wegen eines technischen Defektes der Verschlüsselungsserver neu aus einer Sicherung zu installieren, kann dies alles über den DAKOTA Assistenten ausgeführt werden unter:

EXTRAS – Systemeinst.- FIRMA - DTA§302/§300 – Dakota.le >Verschlüsselungsassistent

8.1 Mail als BCC senden

In der DAKOTA Software können Sie Einstellen, dass sie eine Blindkopie der versendeten Daten automatisch an Ihre eigene Mailadresse gesendet wird unter:

DAKOTA->Konfiguration->Verschlüsselung

[x] Einstellungen für E-Mail Blindkopien

Mit setzten des Hakens können eine, oder mehrere Mailadressen mit „;“ (Semikolon getrennt) eingegeben werden an welche eine Kopie der versendeten Daten geschickt werden soll.

8.2 Ablaufdatum als Wiedervorlage setzen

In der Dakota Software finden Sie unter:

EXTRAS – Schlüsselverwaltung

das Ablaufdatum des derzeitigen Schlüssels
Damit Sie einen Hinweis erhalten wann das Zertifikat Ihres Schlüssels abläuft setzten Sie dieses Datum in mmOrthosoft® auf Wiedervorlage. Legen Sie hierfür die Adresse der ITSG im Ordner Vertriebsadressen an klicken dann auf:

Kalendersymbol -Wiedervorlage

Setzen Sie die Wiedervorlage ca. 2 Wochen VOR dem eigentlichen Ablaufdatum.

WICHTIGER HINWEIS:

Bedenken Sie, dass Sie ab dem Moment des versenden des neuen Antrags bis zum erneuten Einlesen des Zertifikats KEINEN gültigen Schlüssel besitzen und keine Abrechnung versenden können. Daher ist es Empfehlenswert, die letzte

Abrechnung noch durchzuführen und direkt danach einen neuen Antrag zu stellen.

8.3 Annahmestellen (Physikalische IK)

Es gibt nur etwas mehr als eine Handvoll Annahmestellen zu denen 302 Abrechnungsdaten hingeschickt werden können. Die Annahmestellen werden in mmOrthosoft® in Form der Physikalischen IK Nummer hinterlegt. Zur Erleichterung bzw. zur Kontrolle der Eingabe der physikalischen IK in den mmOrthosoft® Krankenkassen kann man diese in der Dakota Software einsehen unter:

DAKOTA - STAMMDATEN – Annahmestellen anzeigen

8.4 Stammdaten aktualisieren

Die Dakota Stammdaten sollten in regelmäßigen Abständen aktualisiert werden unter:

DAKOTA - STAMMDATEN – Stammdaten aktualisieren

Es wird empfhohlen nach dem aktualisieren eine Sicherung durchzuführen

DAKOTA - Zertifikate – Sicherung erstellen

9 DAKOTA Schlüsselzertifikat verlängern

Wie schon erwähnt ist es sinnvoll, das Ablaufdatum des Zertifikats im mmOrthosoft® auf Wiedervorlage zu setzten, damit man rechtzeitig vor dem Ablauf die Verlängerung beantragen kann.
Berücksichtigen Sie, dass Sie zwischen der Neubeantragung und dem Einlesen des Schlüssels (ca. 4-8 Tage) KEINE Daten an die Kassen versenden können. Planen Sie daher eine Neubeantragung immer unmittelbar NACH der letzten Monatsabrechnung ein.

Ihre Stammdaten für den Zertifizierungsantrag und Ihr Schlüssel werden erstmalig bei der ERST-Inbetriebnahme vor der Schlüsselgenerierung von Ihnen erfasst. 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?
· Läuft Ihr Zertifikat in Kürze aus und Sie möchten Ihr Zertifikat beim Trust Center verlängern?

Gehen Sie wie folgt vor:

Starten Sie DAKOTA aus mmOrthosoft® über

EXTAS - Systemeinst - Firma - DTA§302/§300 - Daktota.le -Verschlüsselungsassistent

Ist Ihr Schlüssel schon abgelaufen werden Sie direkt gefragt ob Sie einen neuen beantragen möchten. Folgen Sie den Anweisungen am Bildschirm. Die Vorgehensweise ist die gleiche wie im Kapitel
DAKOTA Konfigurieren beschrieben
nur das die Antragsdaten in der Regel schon ausgefüllt sind und nur noch auf Korrekktheit überprüft werden müssen.

Manuell starten Sie die Beantragung eines neuen Zertifikats in der DAKOTA Software über:

DAKOTA > Zertifikate > Neues Zertifikat beantragen

10 DAKOTA uminstallieren

Bei der Installation bzw. Verlängerung des DAKOTA Schlüssels wird als letzter Schritt immer eine SICHERUNG des aktuellen Schlüssels durchgeführt. Die Sicherung sollte auf einem Netzlaufwerk, am besten in das mmOrthosoft® Verzeichnis, abgelegt werden, damit der Schlüssel in die Tagessicherung des Systems einfließt.

Durch defekte Hardware, Standortwechsel, installieren einer weiteren Version von DAKOTA auf einem 2. Computer usw. kann es notwendig werden, dass die DAKOTA Verschlüsselungssoftware uminstalliert werden muss. Um die Kosten zu vermeiden die durch einen neuen Schlüsselantrag entstehen würden ist es sinnvoll bei der Installation auf den gesicherten Schlüssel zuzugreifen und diesen wieder ein zu lesen.

Die Vorgehensweise absolut identisch wie bei der Neuinstallation beschrieben.

- Holen Sie sich die DAKOTA Software aus der mmOrthosoft® Mailbox
- Rufen Sie das DAKOTA SETUP auf über:

EXTRAS->Systemeinst->Firma->DTA§302/§300->DAKOTA->Setup

- Danach gehen Sie NICHT WEITER um einen neuen Zertifizierungsantrag auszufüllen sondern klicken Sie auf die Funktion
- **SICHERUNG IMPORTIEREN** und laden die Sicherung aus dem Sicherungsverzeichnis

Danach sollte DAKOTA wieder komplett funktionsfähig laufen