Abrechnung per DTA

Welche technischen Voraussetzungen müssen vorhanden sein und wie werden die Daten übermittelt?

Entscheiden Sie sich für die Abrechnung per Datenträger, Datenfernübertragung dgl., wenden Sie sich an eine EDV-Firma Ihres Vertrauens. Sie ist Ihnen sicherlich bei der Beratung der erforderlichen Hard- und Software behilflich.

Sie benötigen für die Durchführung des maschinellen Datenaustausches ein Softwareprodukt, das in der Lage ist, die in den Technischen Anlagen zur Datenübermittlungsvereinbarung definierten Datenstrukturen (EDIFACTFormat) zu liefern und anzunehmen. Informationen über geprüfte Abrechnungssoftware erhalten Sie von:

Informationstechnische Servicestelle der gesetzlichen Krankenversicherung GmbH,Postfach 50 01 52, 63094 Rodgau.

Tel. 0 61 06/8 52 60, Fax 0 61 06/85 26 30

oder von der DAV.

Für die Übermittlung der Daten soll laut Technischer Anlage die Datenfernübertragung (DFÜ) genutzt werden. Soweit die Datenfernübertragung aus technischen oder wirtschaftlichen Gründen nicht realisiert werden kann, können Datenträger verwendet werden. Die technischen Voraussetzungen für eine Übermittlung per DFÜ sind ein Telefon, ein ISDN- Anschluß ein oder ein X400- Anschluß, ein PC mit ISDN-Karte, X400 oder Modem und eine geeignete Software, die imstande ist, die Daten zu verschlüsseln und gemäß den zulässigen Standards FTAM bzw. X.400 oder per EMAIL zu übertragen.

Wie funktioniert die Verschlüsselung?

Voraussetzung für den elektronischen Datenaustausch mit personenbezogenen Daten ist, daß die Vertraulichkeit, die Integrität und die Verbindlichkeit der Daten sichergestellt sind. Dies geschieht durch Verschlüsselung und digitale Signatur auf der Grundlage kryptographischer Verfahren. Dadurch ist gewährleistet, daß die datenschutzrechtlichen Bestimmungen eingehalten werden.
Jeder Teilnehmer am Datenaustausch verfügt dazu über ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten (geheimen) Schlüssel. Der private ist nur dem Schlüsseleigner bekannt; der öffentliche Schlüssel dagegen wird von den TrustCentern allgemein publik gemacht.

Die beiden Schlüssel eines Teilnehmers stehen in einer besonderen Beziehung zueinander. Daten, die mit einem Schlüssel verschlüsselt werden, können nur mit dem anderen wieder entschlüsselt werden. Der absendende Kommunikationspartner verschlüsselt mit dem öffentlichen Schlüssel des Empfängers Daten, die nur der Empfänger als Inhaber des dazugehörigen privaten Schlüssels wieder entschlüsseln kann. Mit diesem können jedoch Daten nicht nur ent- sondern auch verschlüsselt werden. Man spricht in diesem Fall von digitaler Signatur oder elektronischer Unterschrift. Mit dem allgemein bekannten öffentlichen Schlüssel des absendenden Teilnehmers kann jeder die digitale Signatur prüfen. Sie übernimmt somit die Funktion einer eigenhändigen Unterschrift. Darüber hinaus können durch Prüfung der digitalen Signatur Fälschungen der Daten zuverlässig erkannt werden.

Durch die Kombination von Verschlüsselung und digitaler Signatur wird sichergestellt, daß Daten vertraulich übermittelt werden können, der Absender der Daten zuverlässig erkannt und die Unverfälschtheit der übertragenen Daten festgestellt werden kann.

Für den Schutz seines privaten Schlüssels ist jeder Beteiligte selbst verantwortlich. Die Authentizität des öffentlichen Schlüssels muß von einer neutralen und vertrauenswürdigen Instanz, dem sogenannten TrustCenter, durch ein Zertifikat bestätigt werden.

Wie erfolgt die Zertifizierung?

Sie erzeugen sich mit Hilfe Ihrer Verschlüsselungssoftware (i. d. R. Bestandteil der Übermittlungssoftware) einen Schlüssel und senden diesen an:

ITSG-TrustCenter
Postfach 12 30
49702 Meppen
Tel. 0 59 31/8 05-2 83
Fax 0 59 31/8 05-1 00
E-Mail: tc@itsg.de

Das TrustCenter hat die Aufgabe, allen Teilnehmern am Datenaustausch authentische öffentliche Schlüssel bereitzustellen. Dazu muß sich das TrustCenter von der Identität des Inhabers eines öffentlichen Schlüssels überzeugen.

Wie erfolgt die technische Anbindung?

Um mit der AOK Bayern Daten per DFÜ austauschen zu können, tragen Sie unsere Datenannahme- und Verteilstelle in Ihrem eigenen Übermittlungssystem als DFÜ-Partner ein. Die dafür erforderlichen Angaben können Sie einem Datenblatt entnehmen, das Ihnen die DAV vorab zusendet.

Bitte ergänzen Sie dieses Datenblatt um Ihre relevanten Daten und senden Sie es wieder an die DAV zurück, damit auch wir Sie als Partner in unserem System generieren können.

Für den ersten technischen Anbindungstest ist es nicht erforderlich, daß dazu bereits fachliche Daten entsprechend der Datenübermittlungsvereinbarung in EDIFACT-Struktur vorliegen. Die technische Anbindung kann auch mit einer kleinen Textdatei erfolgen, die man sich gegenseitig übermittelt. Der technische Teil der Anbindung gilt als abgeschlossen, sobald beiderseits verschlüsselte Daten ausgetauscht worden sind.

Bei Fragen oder Problemen sind Ihnen die Ansprechpartner in unserer DAV gerne behilflich.

Testverfahren

Während des Testverfahrens muß zusätzlich zu den Daten eine gleichlautende Papierrechnung an das DLZ - gekennzeichnet mit " DTA-Test" - gestellt werden.
Diese darf erst nach einer dementsprechenden Nachricht durch das DLZ weggelassen werden! Dies geschieht in der Regel dann, wenn eine fehlerfreie maschinelle Übermittlung und eine gute Datenqualität das Parallelverfahren überflüssig machen.

Das Testverfahren ist für alle AOKs bundesweit gültig, es muß daher nicht mit jeder einzelner AOK durchgeführt werden.

Übersicht über den chronologischen Ablauf des maschinellen Testbetriebes:

1. Kontaktaufnahme mit der Datenannahme- und Verteilstelle (DAV), *2.* Realisierung der technischen Voraussetzungen zur maschinellen Datenübermittlung,

3. Durchführung der Schlüsselzertifizierung,

4. Testen der technischen Anbindung mit der DAV,

5. Anlieferung der zusätzlichen Papierrechnung, gekennzeichnet mit " DTATest" sowie der Verordnungen an das DLZ.

6. Nach erfolgter telefonischer Nachricht des DLZ zum Beenden der Testlieferungen Übergang zum Echtverfahren und Wegfall der zusätzlichen Papierrechnung.

Stand: 11.01.2008