Leistungsbeschreibung – dakota.le

dakota.le ist ein Programm zur Unterstützung der gesicherten Internet-Kommunikation zwischen Leistungserbringern und den gesetzlichen Krankenkassen. Die Auflagen, 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. dakota.le ist eine Produktfamilie der ITSG GmbH und steht für 'Datenaustausch und Kommunikationen auf der Basis Technischer Anlagen'.

Grundlagen
Die Anforderung an den Datenaustausch zwischen Leistungserbringern und den gesetzlichen Krankenkassen sind in §§294 ff. SGB V geregelt. Der GKV Spitzenverband hat mit den Spitzenverbänden der Leistungserbringer Verträge geschlossen bzw. Richtlinien erstellt. Die Dokumentation hierzu steht den Beteiligten zur Verfügung. Vorrangig wird der Kommunikationsweg über das Internet mittels E-Mail für den Versand genutzt.

Das Sicherheitsverfahren im Gesundheitswesen
Voraussetzung für den elektronischen Datenaustausch personenbezogener Daten ist, dass Vertraulichkeit, Integrität und Verbindlichkeit in gleicher Weise sichergestellt werden wie beim bisherigen 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 gemacht. 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. Die 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 Daten nicht nur entschlüsselt, sondern auch verschlüsselt werden. Man spricht in diesem Fall von digitaler Signatur. Der Absender signiert Daten mit seinem privaten Schlüssel, mit Hilfe des allgemein bekannten öffentlichen Schlüssels des Absenders kann die digitale Signatur überprüft werden. 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 wird,
- die Unverfälschtheit übertragener 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 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 sogenannten Trust Center, durch ein Zertifikat bestätigt werden.

Das Produkt
Eine wesentliche Vereinfachung für die Umsetzung der technischen Aufgabenstellung bietet das Produkt dakota.le. Diese Softwarelösung unterstützt die Vorgaben für den Datenaustausch und stellt die erforderlichen Funktionen bereit für die

- Prüfung der Datenlieferung
- Verschlüsselung der Datenlieferung
- Datenfernübertragung mittels E-Mail

dakota.le ist ein Kommunikationsprogramm, das speziell auf die Anforderungen des verschlüsselten Datenaustausches mit den gesetzlichen Krankenkassen und den dafür vorgeschriebenen Rahmenbedingungen ausgerichtet ist. Das Programm nutzt eine neutrale Schnittstelle zur Übernahme der Dateien mit den Abrechungsdaten aus den vorgeschalteten Fachprogrammen. Die Fachanwendung stellt die zu übertragenden Daten in einem vorgegebenen Dateibereich zum Versand zur Verfügung. dakota.le führt eingeschränkte Prüfungen durch, um bereits vor dem Versand fehlerhafte Dateien zu erkennen. Die Dateien mit den Nutzdaten werden vollständig verschlüsselt. Die erforderlichen Steuerdaten werden in einer zugehörigen Auftragsdatei geliefert, die von der jeweiligen Fachanwendung zu erstellen ist. Die zu einer Lieferung gehörenden Dateipaare werden automatisch per E-Mail an die zuständigen Annahmestellen der Krankenkassen gesandt. dakota.le zeichnet sich durch eine einfache Bedienung aus. Die ganze Verarbeitung wird über nur zwei Funktionen – Verschlüsseln und Versenden – gesteuert. Durch das komplexe Thema der Datensicherheit wird der Anwender mit Hilfe eines Assistenten geführt. Schritt für Schritt werden alle notwendigen Aktionen per Mausklick erledigt. Jederzeit kann der Status der Verarbeitung über die übersichtlichen Protokolle abgerufen werden. Eine funktionsorientierte Hilfe gibt gezielt Auskunft, was zu tun ist. Darüber hinaus kann dakota.le direkt von der Fachanwendung aufgerufen werden, dakota.le wird quasi ferngesteuert. Für diese Betriebsart sind keine Benutzereingaben im laufenden Betrieb mehr nötig.

Technische Beschreibung
Das Programm ist modular aufgebaut. Die einzelnen Module können ohne wesentliche Beeinflussung der anderen Module an sich ändernde Vorgaben angepasst werden.

MODUL - Prüfen Auftragsdatei
Die von der Fachanwendung erstellte Auftragsdatei wird nach den Vorgaben der technischen Richtlinien für den Datenaustausch geprüft. Sofern Fehler erkannt werden, wird die Weiterverarbeitung des betreffenden Dateipaares (Nutzdaten und Auftragssatz) gestoppt und ein Fehlerhinweis gegeben.

MODUL - Verschlüsselung
Um den Vorgaben der Security-Schnittstelle im Gesundheitswesen zu entsprechen, wird in dakota.le ein kryptographisches Toolkit eingesetzt. Dieses basiert auf den Standards von PKCS#7 (Public Key Cryptography Standards)

dakota.le setzt die folgenden Aufgaben in Form eines Assistenten, mit Routinen des Toolkits um:

- Erzeugen eines öffentlichen und privaten Schlüssels: Aus Daten des Arbeitgebers kombiniert mit einer errechneten Zufallszahl wird eine einmalige Kombination zur Schlüsselerzeugung gewonnen.

- Zertifizierung zum Trust Center: Zur Teilnahme am öffentlichen Schlüsselverfahren ist es notwendig, den eigenen öffentlichen Schlüssel dem Teilnehmerkreis zur Verfügung zu stellen und die öffentlichen Schlüssel aller Annahmestellen zu erhalten.

- Verwaltung der öffentlichen Schlüssel: Das komplette Einlesen der öffentlichen Schlüssel der Kommunikationspartner (z.B. Annahmestellen der Krankenkassen) und ein Update der Schlüsseldateien ist sichergestellt.

- Verschlüsseln der Nutzdaten mit dem entsprechenden Schlüssel der zuständigen Annahmestelle der gesetzlichen Krankenkassen.

MODUL – Kommunikation
dakota.le erstellt E-Mails nach den technischen Richtlinien des Datenträgeraustausches. Die E-Mail besteht aus der Empfängeradresse, Absender, einigen Angaben zur Lieferung, der verschlüsselten Datei und der Auftragsdatei. Die E-Mail wird automatisch an MS Outlook (32 Bit) übergeben oder per

SMTP an den E-Mail-Server übertragen. Alternativ kann die vorbereitete E-Mail per drag-and-drop an ein anderes Mailsystem übergeben werden.

Dateischnittstelle
Der Austausch der Daten zwischen dakota.le und der jeweiligen Fachanwendung erfolgt auf der Basis einer Datei-Schnittstelle. Die für die Sozialversicherung erzeugten Dateien (DEÜV oder Beitragsnachweise) werden in ein definiertes Verzeichnis geschrieben. dakota.le übernimmt diese Dateien aus diesem Bereich.

Systemvoraussetzungen
Standard-PC mit Intel Prozessor, Standard-Drucker, Internet-Anschluss, Microsoft.net Framework 4.8 full Plattenbedarf ca. 50 MB

Betriebssysteme: Windows 10 oder Windows 11

Der Anwender des Produktes sorgt eigenverantwortlich für die korrekte Einrichtung und die Funktion der erforderlichen Hard- und Software sowie den Anschluss an das Internet. Standardmäßig ist eine E-Mail-Schnittstelle zum Produkt MS Outlook (32 Bit) integriert.