Leistungsbeschreibung – dakota.ag

dakota.ag ist ein Programm zur Unterstützung der gesicherten Internet-Kommunikation zwischen Arbeitgebern und der gesetzlichen Sozialversicherung. Die Auflagen, den Datenaustausch zu sichern, werden durch die Vorgaben der Gemeinsamen Grundsätze Technik nach §95 SGB IV erfüllt. Alle Nutzdaten werden vor dem Versand verschlüsselt. dakota.ag ist eine Produktfamilie der ITSG GmbH und steht für 'Datenaustausch und Kommunikationen auf der Basis Technischer Anlagen'.

Grundlagen
Seit dem 1.1.2006 sind die Arbeitgeber verpflichtet, ihre Meldungen nach §28b SGB IV elektronisch abzugeben. In der Zwischenzeit sind diverse verpflichtende elektronische Meldeverfahren hinzugekommen. Die technischen Grundlagen für den Datenaustausch sind in den Gemeinsamen Grundsätzen Technik nach §95 SGB IV festgelegt. Dabei ist in den Arbeitgeber-Meldeverfahren ausschließlich eine Datenübertragung über https zulässig (§17 DEÜV).

Das Sicherheitsverfahren im Gesundheits- und Sozialwesen
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. Daher sind in der Anlage 16 der Gemeinsamen Grundsätze Technik nach §95 SGB IV die Vorgaben zum sicheren Datenaustausch geregelt.
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.ag. Diese Softwarelösung unterstützt die Vorgaben für den Datenaustausch und stellt die erforderlichen Funktionen bereit für die

- Verschlüsselung und Signatur ausgehender Datenlieferungen
- Entschlüsselung und Signaturprüfung eingehender Datenlieferungen
- Datenfernübertragung mittels https

dakota.ag 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 Meldedaten oder mit Beitragsnachweisen aus vorgeschalteten zertifizierten Entgeltabrechnungsprogrammen oder Zeiterfassungssystemen. Die Fachanwendung stellt die zu übertragenden Daten in einem vorgegebenen Dateibereich zum Versand zur Verfügung. dakota.ag führt 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 dokumentiert, die dakota.ag erstellt. Die zu einer Lieferung gehörenden Dateipaare werden automatisch per https an den zuständigen Kommunikationsserver nach §96 SGB IV gesandt. dakota.ag 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.ag direkt von der Lohn- und Gehaltsabrechnung aufgerufen werden, dakota.ag 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 Nutzdaten
Das Programm überprüft die Dateien vor der Weiterverarbeitung. Die erkannten Fehler werden protokolliert und führen ggf. zum Stopp der Weiterverarbeitung. Der Anwender hat die Möglichkeit, aufgrund der angemerkten Fehlerhinweise korrigierend einzugreifen. Heute ist eine einfache Prüfung des Dateinamens und der Vorlaufsätze integriert. Erweiterte Prüfungen sollen ggf. in einer folgenden Produktversion eingebunden werden.

MODUL - Verschlüsselung
Um den Vorgaben der Anlage 16 der Gemeinsamen Grundsätze Technik zu entsprechen, wird in dakota.ag
ein kryptographisches Toolkit eingesetzt.

dakota.ag 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.

- *Entschlüsseln der eingehenden Nutzdaten inklusive der Signaturprüfung.*

MODUL – Kommunikation
dakota.ag erstellt eXTra-Nachrichten nach den Gemeinsamen Grundsätzen Technik. eXTra-Nachrichten werden via https von dakota.ag an den zuständigen Kommunikationsserver übertragen. Zudem werden Rückmeldungen der Sozialversicherungsträger über die eXTra-Schnittstelle von den Kommunikationsservern abgerufen und der erfolgreiche Abruf quittiert.

Dateischnittstelle
Der Austausch der Daten zwischen dakota.ag und der jeweiligen Entgeltabrechnung erfolgt auf der Basis einer Datei-Schnittstelle. Die für die Sozialversicherung erzeugten Dateien (DEÜV oder Beitragsnachweise) werden in ein definiertes Verzeichnis geschrieben. dakota.ag 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: MS Windows 10 und 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 integriert.