Anlage 6

zur Vereinbarung zwischen dem Zentralinstitut für die kassenärztliche Versorgung in der Bundesrepublik Deutschland und der Kassenärztlichen Vereinigung gemäß § 80 SGB X

Anforderungen an das Programm zur Verschlüsselung und Pseudonymisierung von vertragsärztlichen Abrechnungsdaten (VDA)

6.1 Funktionen des Programms

Die Software steuert alle Prozesse der Verarbeitung von XML-Dateien, realisiert unter anderem die Pseudonymisierung von arzt- und patientenbezogenen Attributen sowie die Ver- und Entschlüsselung von Dateien und übernimmt die sichere Übermittlung von Dateien an festgelegte Adressaten.

Insbesondere beinhaltet die Software die nachstehenden Kernfunktionalitäten:

Funktion	Kurze Erläuterung zur Funktion
FKT1	Erstellung von definierten XML-Dateien aus standardisierten Daten der KV (sog. vdx-Schnittstelle) in zwei Dateien. Eine Datei beinhaltet ambulante Diagnosedaten Die zweite Datei enthält arzt- und patientenbezogene Attribute. Eine spätere Zusammenführung wird durch eine eindeutige interne laufende Nummer sichergestellt.
FKT2	Verschlüsselung von Dateiinhalten (Hybridverfahren)
FKT3	Entschlüsselung von Dateiinhalten (Hybridverfahren)
FKT4	Komprimierungs- bzw. Dekomprimierungsfunktion
FKT5	Digitale Signierung von Datenpaketen zur Sicherstellung der Authentizität und Integrität
FKT6	Überprüfung von digitalen Signaturen von empfangenen Datenpaketen zur Sicherstellung der Authentizität und Integrität
FKT7	Doppelte Pseudonymisierung (RIPEMD-160)
FKT8	Logfile-Mechanismus
FKT9	Archivverschlüsselung eventueller Notwendigkeit der Respeudonymisierung
FKT10	Datenversand mittels SSH-Tunnel

6.2 Einsatzorte der Software mit entsprechendem Funktionsumfang

Einsatzort (Name der Institution)	Funktion (siehe Kernfunktionalität)
Kassenärztlichen Vereinigungen (KV)	FKT1, FKT2, FKT4, FKT5, FKT8, FKT10
Vertrauensstelle (DSSG mbH)	FKT2, FKT3, FKT4, FKT5, FKT6, FKT7, FKT8, FKT9, FKT10
Datenstelle im Zentralinstitut (ZI)	FKT3, FKT4, FKT6, FKT8

6.3 Systemvoraussetzungen

Die Software kann auf Windows System oder auf Linux / UNIX System unter Vorraussetzung einer installierten Java Runtime Environment (mind. Version 1.5 oder höher) betrieben werden. Der eingesetzte Rechner sollte nur über minimal benötigte Dienste des Betriebssystems verfügen und muss derart konfiguriert werden, dass eine zertifikatsbasierte SSH-Verbindung zur Kommunikation aufgebaut werden kann. Diese wird für die Übertragung der signierten und verschlüsselten Dateien verwendet. Die Authentisierung der Kommunikationspartner erfolgt per Public-Key-Authentisierung.

Weitere Angaben zu den Verfahren zur Authentifizierung, Verschlüsselung und Pseudonymisierung finden sich in Anlage 8.