Anlage 5

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 Arzneiverordnungsdaten (VPA)

5.1 Funktionen von VPA

Die VPA-Software (VPA – Verschlüsselung und Pseudonymisierung von Arzneiverordnungsdaten) steuert alle Prozesse der Verarbeitung, realisiert unter anderem die Pseudonymisierung von arzt- und patientenbezogenen Attributen, nimmt die Ver- und Entschlüsselung von Dateien vor und übernimmt die sichere Übermittlung von Dateien an festgelegte Adressaten.

Insbesondere beinhaltet VPA die nachstehenden Kernfunktionalitäten:

Funktion	Kurze Erläuterung zur Funktion
FKT1	Zeilenweise Aufteilung von CSV-Dateien unter Vorgabe eines gemeinsamen, zeilenorientierten eindeutigen Schlüssels zur Rekonstruktion, d.h. eine CSV-Datei wird in zwei Dateien aufgespalten. Eine Datei beinhaltet medizinische Falldaten zu Arzneiverordnungen und die zweite Datei enthält arzt- und patientenbezogene Attribute. Dabei wird die spätere Zusammenführung durch die Vergabe einer eindeutigen Zuordnungs-ID pro Zeile 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

5.2 Einsatzorte von VPA mit entsprechendem Funktionsumfang

Einsatzort (Name der Institution)	Funktionen (siehe VPA Kernfunktionalitäten)
Apothekenrechenzentren (ARZ)	FKT1, FKT2, FKT4, FKT5, FKT8, FKT10
Vertrauensstelle (DSSG mbH)	FKT2, FKT3, FKT4, FKT5, FKT6, FKT7, FKT8, FKT9, FKT10
Datenstelle des Zentralinstitut (ZI)	FKT2, FKT3, FKT4, FKT5, FKT6, FKT8, FKT10
Kassenärztlichen Vereinigungen (KV)	FKT3, FKT4, FKT6, FKT8

5.3 Systemvoraussetzungen von VPA

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.