Anlage 8

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

Verfahrensbeschreibung zur Authentifizierung, Verschlüsselung und Pseudonymisierung

Um der hohen Schutzbedürftigkeit und der gesetzlich geforderten Pseudonymisierung bei der Datenbereitstellung nach § 300 Absatz 2 SGB V durch das Zentralinstitut im Auftrag der KVen nachzukommen, werden folgende Verfahren verwendet:

1. Verfahren zur Authentifizierung
Zur sicheren Authentifizierung bei der SSH-Verbindung zwecks automatisierten Datentransfers zwischen Apothekenrechenzentrum mit Vertrauensstelle, Vertrauensstelle mit ZI-Datenstelle und ZI-Datenstelle mit KV wird das sog. Public-Key-Verfahren verwendet. Die Schlüssel werden durch ein externes zertifiziertes Trustcenter erstellt und beglaubigt. Die Schlüssel haben eine Schlüssellänge von 2048 Bit und besitzen eine Gültigkeit von einem Jahr. Die Verbindung mittels SSH und der Datentransfer wird automatisiert durch die Eigensoftware VPA durchgeführt.

Alle beteiligten Institutionen werden vertraglich verpflichtet, das Schlüsselmaterial sicher zu verwahren und nach Ablauf ihrer Gültigkeit unwiderruflich zu vernichten. Das ZI stellt sicher, dass die Einrichtung nach Ablauf der Gültigkeit der asymmetrischen Schlüssel neue Schlüssel durch das Trustcenter erhält. Das Schlüsselmaterial wird vom Trustcenter auf CD mittels Postidentverfahren bereitgestellt.

2. Verfahren zur Verschlüsselung
Es werden zwischen den genannten Institutionen nur verschlüsselte Datenpakete übertragen. Die Verschlüsselung wird automatisiert durch die Eigensoftware VPA durchgeführt. Zur Verschlüsselung wird das Hybridverfahren verwendet. Hierbei kommt das Verfahren AES-256 zum Einsatz. Der zur symmetrischen Verschlüsselung verwendete 256 Bit lange Schlüssel wird für jede Datei und jede Datenlieferung einmalig und zufällig durch VPA erzeugt. Der symmetrische Schlüssel wird mit dem 2048 Bit langem öffentlichen Schlüssel der Empfängerinstitution nach dem Verfahren RSA verschlüsselt und kann nur durch den privaten Schlüssel der Empfängerinstitution entschlüsselt werden. Somit wird sichergestellt, dass z.B. die Vertrauensstelle nur die für die Pseudonymisierung vorgesehene Hauptdatei Stammdaten (siehe Anlage 2) entschlüsseln und verarbeiten kann, während die Hauptdatei Falldaten (siehe Anlage 2) durch die Vertrauensstelle nicht entschlüsselt werden kann.

Alle beteiligten Institutionen werden vertraglich verpflichtet, das Schlüsselmaterial sicher zu verwahren und nach Ablauf ihrer Gültigkeit unwiderruflich zu vernichten. Das ZI stellt sicher, dass die Einrichtung nach Ablauf der Gültigkeit der asymmetrischen Schlüssel neue Schlüssel durch das Trustcenter erhält. Das Schlüsselmaterial wird vom Trustcenter auf CD mittels Postidentverfahren bereitgestellt.

3. Verfahren zur Signatur von Datenpaketen
Alle zu übertragenen Dateien werden von der Versenderinstitution digital signiert. Die Signierung einer Datei erfolgt mit dem Hash-Algorithmus SHA-256 und dem privaten Schlüssel der Versenderinstitution. Auf Empfängerseite wird die Signatur auf korrekte Herkunft mit dem öffentlichen Schlüssel der Versenderinstitution überprüft. Die Signierung von Dateien und die Überprüfung von Signatur wird durch die Eigensoftware VPA sichergestellt.

Alle beteiligten Institutionen werden vertraglich verpflichtet, das Schlüsselmaterial sicher zu verwahren und nach Ablauf ihrer Gültigkeit unwiderruflich zu vernichten. Das ZI stellt sicher, dass die Einrichtung nach Ablauf der Gültigkeit der asymmetrischen Schlüssel neue Schlüssel durch das Trustcenter erhält. Das Schlüsselmaterial wird vom Trustcenter auf CD mittels Postidentverfahren bereitgestellt.

4. Verfahren zur Pseudonymisierung

Zur Wahrung der Persönlichkeitsrechte werden in der Hauptdatei Stammdaten (siehe Anlage 2) patient- bzw. arztidentifizierbare Inhalte durch die Vertrauensstelle pseudonymisiert. Dazu wird ein zweistufiges Verfahren angewendet. In der ersten Phase werden die Klartextangaben zu Versicherten- bzw. Arztkennung mit einem ersten Geheimnis pseudonymisiert. Das entstandene Pseudonym wird in einer zweiten Phase mit einem weiteren Geheimnis, welches für die KVen und das ZI unterschiedlich ist, pseudonymisiert. Die Geheimnisse zur Pseudonymisierung werden in einem sog. HSM (Hardware-Sicherheitsmodul) erzeugt. Auf beiden Stufen wird das RIPEMD-160 Verfahren angewendet. Im ersten Schritt werden bei jeder Pseudonymisierung Mappingtabellen erzeugt, die auf ein externes optisches Medium gesichert werden. Es erfolgt keine dauerhafte Speicherung der Mappingtabelle im IT-Verbund der Vertrauensstelle. Die erzeugten Mappingtabellen werden außerhalb der Vertrauensstelle an einem sicheren Ort (Banksafe) verwahrt. Die Mappingtabellen werden dabei verschlüsselt gespeichert. Der hierzu verwendete Schlüssel wird zufällig und zur einmaligen Verwendung im HSM erzeugt. Das fortlaufende Wegschreiben der Mappingtabellen stellt sicher, dass zu einem späteren Zeitpunkt, z.B. weil das Verfahren zur Pseudonymisierung korrumpiert wurde oder als überaltert gilt, eine Neupseudonymisierung nach Umstellung des Verfahrens möglich ist. Das HSM ist der zentrale Ort der Verwahrung der Geheimnisse zur Pseudonymisierung, der Geheimnisse für die Verschlüsselung der Mappingtabellen und des verwendeten Schlüsselmaterials für das Verfahren der Verschlüsselung und Signierung der Datenpakete. Es stellt sicher, dass diese Geheimnisse nicht extrahiert werden können. Detaillierte Angaben zur Funktionsweise des HSM finden sich im Sicherheitskonzept der Vertrauensstelle. Die Pseudonymisierung wird automatisiert durch die Eigensoftware VPA durchgeführt.

Alle beteiligten Institutionen werden vertraglich verpflichtet, die das Schlüsselmaterial sicher zu verwahren und nach Ablauf ihrer Gültigkeit unwiderruflich zu vernichten. Das ZI stellt sicher, dass die Einrichtung nach Ablauf der Gültigkeit der asymmetrischen Schlüssel neue Schlüssel durch das Trustcenter erhält. Das Schlüsselmaterial wird vom Trustcenter auf CD mittels Postidentverfahren bereitgestellt.

Schematische Darstellung der Pseudonymisierung:

1. Phase der Pseudonymisierung

P = H (M)

P	Pseudonym Phase 1
H	Anwendung RIPEMD-160 und ein geheimes Kennwort
M	Klartext

Lieferung für ZI-Datenstelle

Folgende Klartextangaben werden pseudonymisiert:

- Betriebsstättennummer (BS_NR)
- Arztnummer (LA_NR)
- Versichertennummer (PAT_NR) falls PAT_NR nicht vorhanden wird der PAT_VORNAME und PAT_NACHNAME pseudonymisiert

Lieferung KV

Folgende Klartextangabe wird pseudonymisiert:

- Versichertennummer (PAT_NR) falls PAT_NR nicht vorhanden wird der PAT_VORNAME und PAT_NACHNAME pseudonymisiert

2. Phase der Pseudonymisierung

Lieferung ZI

P_{ZI} = H (P)

P	Pseudonym Phase 1
H	Anwendung RIPEMD-160 und ein geheimes Kennwort für die Pseudonymisierung der ZI-Lieferung
P_{ZI}	Pseudonym Phase 2 für ZI-Datenstelle-Datei

Lieferung KV

P_{KV} = H (P)

P	Pseudonym Phase 1
H	Anwendung RIPEMD-160 und ein geheimes Kennwort für die Pseudonymisierung der KV-Lieferung
P_{ZI}	Pseudonym Phase 2 für KV-Datei

5. Verfahren zur Sicherstellung der Nachweisbarkeit von Datenlieferungen

Die erfolgten Auslieferungen und Empfänge der Datenpakete zwischen den beteiligten Einrichtungen werden nachvollziehbar protokolliert. Zu diesem Zweck wird nach erfolgreicher Übermittlung eines Datenpaketes auf Versenderseite ein Sendebericht erstellt. Dieser Sendebericht enthält das Versanddatum, den Namen des versendeten Datenpaketes und den Hashwert der Signatur. Dieser Sendebericht wird als Datei auf Senderseite archiviert. Auf Empfängerseite wird eine

Empfangsbestätigungsdatei erzeugt. Diese beinhaltet Empfangsdatum, Hashwert der Signatur und einen Verarbeitungs- und Signaturstatus. Die entsprechende Datei wird auf Empfängerseite archiviert und mittels Emailverfahren an die Versenderseite übermittelt.

6. Verfahrensbeschreibung zur Datenübermittlung

Die Kommunikation zwischen Apothekenrechenzentrum und Vertrauensstelle sowie zwischen Vertrauensstelle und ZI-Datenstelle erfolgt auf Basis von SSH unter Anwendung des Verfahrens AES-256. Die eigentliche Dateiübertragung wird mit dem SSH File Transfer Protocol (SFTP) durchgeführt. Hierbei ist eine SSH-Implementierung zu verwenden, die eine registrierte OID aufweist. Die Datenübertragung zwischen ZI-Datenstelle und KV erfolgt über FTP mit VPN-Tunnel.

Zusätzliche organisatorische und technische Maßnahmen wie z.B. Verwenden eines Schleusenprinzips bei der Datenannahme, Datenverarbeitung und Datenweiterleitung oder der Erzeugung von log-Dateien bei der Datenverarbeitung, etc. sowie die weitere Details der oben beschriebenen Verfahren sind in dem Sicherheitskonzept der Vertrauensstelle bzw. dem Sicherheitskonzept der ZI-Datenstelle beschrieben.