Kurzgutachten für die Rezertifizierung des Produkts PKV-Pseudodatenpool V 1.0 der Firma trusted documents GmbH nach der DSAVO Schleswig-Holstein

1. Zeitpunkt der Prüfung

Dezember 2008 bis September 2010

2. Grund der Rezertifizierung – Änderungen des Produkts

Die Rezertifizierung des Produkts PKV-Pseudodatenpool V 1.0 war zum Einen wegen des Ablaufs der Zertifizierung und zum Anderen wegen der nun erfolgten Einbeziehung der Clientmodule in die Zertifizierung erforderlich geworden. Das am 24. Juni 2008 zertifizierte Produkt PKV-Pseudodatenpool V 1.0 selbst ist unverändert geblieben. Die im Gutachten, das der Zertifizierung vom Juni 2008 zu Grunde liegt, getroffenen Feststellungen gelten unverändert weiter. Die Dauer der Rezertifizierung ergab sich dadurch, dass während des Zertifizierungsprozesses noch eine Optimierung bei der Implementierung der Verschlüsselung vorgenommen wurde. Die Neuerungen beziehen sich auf die Clientsysteme (zu deren technischen Beschreibung vgl. Ziff. 6.2.2).

3. Adresse des Antragstellers

trusted documents GmbH
Karl-Martell-Straße 60
D-90431 Nürnberg

4. Adresse des Sachverständigen (technischer und rechtlicher Gutachter)

Dipl. Informatiker Werner Hülsmann
Datenschutzconsulting.info
Obere Laube 48
78462 Konstanz
Tel.: 07531 / 365 90 54
E-Mail: wh@d-s-c.info
URL: http://www.d-s-c.info

5. Kurzbezeichnung des IT-Produktes

PKV-Pseudodatenpool V 1.0 – PKV-Pseudodaten-Pool – bürgerfreundlicher (PKV-) Rechnungsdatenaustauch (brda), (basierend auf einer Erfindung von Robert Niggl).

6. Detaillierte Bezeichnung des IT-Produktes

PKV-Pseudodatenpool V 1.0 – PKV-Pseudodaten-Pool – bürgerfreundlicher (PKV-) Rechnungsdatenaustauch (brda), (basierend auf einer Erfindung von Robert Niggl) – Poolsystem und Clientsysteme. Prüfungsgegenstand ist der PKV-Pseudodatenpool V 1.0 mit seinen Schnittstellen und der Rahmenvertrag zwischen dem Betreiber und seinen Vertragspartnern sowie und die Clientsysteme bestehend jeweils aus Client 1 und Client 2 (vgl. Abbildung 2a). Das im Juni 2008 zertifizierte Kernsystem (vgl. Zertifikat 4-6/2008), der eigentliche Pseudodatenpool blieb dabei unverändert.

6.1. Allgemeine Beschreibung

trusted documents betreibt eine Infrastruktur-Lösung im Bereich der privaten Krankenversicherungen (PKV) für den gesicherten Austausch von Abrechnungsdaten zwischen den Leistungserbringern bzw. deren Abrechnungsdienstleistern und den mittelbar am Abrechnungsprozess beteiligten Zahlstellen (PKV-Unternehmen, Beihilfestellen). Verfahrensbeteiligte sind dabei: niedergelassene Ärzte, Heilpraktiker, Therapeuten, Privatärztliche Verrechnungsstellen (PVS), Arztsoftwarehersteller, Portale, Gateways, sowie Softwarehersteller für Verschlüsselung und Zahlstellen. Die Rechungsdaten werden dabei durch eine PVS oder ein Portal für Leistungserbringer über einen speziellen Verschlüsselungsalgorithmus mit einem Einmalschlüssel verschlüsselt und der Einmalschlüssel im Datenpool abgelegt. Der Poolbetreiber hat somit keinerlei Zugriff auf die Rechnungsdaten selbst.

Mögliche Kunden des Poolbetreibers sind PKV-Unternehmen und Beihilfestellen. Diese Kunden können über ein Gateway aus dem PKV-Pseudodatenpool den zur Entschlüsselung der ihnen vom Betroffenen über einen Datamatrixcode weitergegebenen verschlüsselten Rechnungsdaten erforderlichen Einmalschlüssel aus dem Pool auslesen. Mit Hilfe einer speziell entwickelten Decodingsoftware können die Kunden dann die Rechnungsdaten entschlüsseln und in ihren Dokumentenworkflow einspeisen.

Über den Rahmenvertrag (vgl. Anlage_1_-_Rahmenvertrag_g4_1.pdf des Gutachtens vom Juni 2008) wird sichergestellt, dass alle Vertragspartner nur zertifizierte und

vom Poolbetreiber abgenommene Clientsysteme einsetzen dürfen. Im Rahmen dieser Rezertifizierung werden nun die entsprechenden von trusted documents zur Verfügung gestellten Clientsysteme ebenfalls begutachtet.)

6.2. Technische Beschreibung

6.2.1. Pseudodatenpool

Für den PKV-Pseudodatenpool V 1.0 von trusted documents wird J2EE als Technologieplattform eingesetzt, wobei aus Gründen der Security und Skalierbarkeit zusätzlich der Apache Webserver zum Einsatz kommt. Der Apache Webserver dient dazu, den Internetauftritt für Trusted documents zu hosten und um Loadbalancing auf die Applikationsserver zu ermöglichen. Als Middleware wird ein JBoss-Applikationsserver mit einem Web- und einem EJBContainer eingesetzt. Dieser EJB-Container bildet auch die Schnittstelle zur relationalen Datenbank. Die Datenübermittlung durch PVS und die Abholung der Daten durch Versicherungsunternehmen erfolgt über eine AES-256 verschlüsselte Verbindung. Die Ver- und Entschlüsselung des SSL-Datenstroms übernimmt ein Apache-Webserver. Hierdurch wird eine vertrauliche Datenübertragung sichergestellt.

Die Erst-Verschlüsselung der Rechnungsdaten selbst erfolgt mit dem Onetimepad-Verfahren unter Verwendung der XOR (Exklusive ODER)-Verschlüsselung. Bei dem eingesetzten Onetimepad-Verfahren wird im Clientsystem des Rechnungserstellers (dies kann der Leistungserbringer selbst, eine PVS oder ein Portal sein) für jede Verschlüsselung einer Rechnung mit Hilfe eines Zufallgenerators ein ausreichend langer Einmalschlüssel erzeugt.

Die verschlüsselten Daten und der dazugehörige Einmalschlüssel werden auf zwei verschiedenen und unabhängigen Wegen transportiert: Die mit dem Einmalschlüssel verschlüsselten Rechnungsdaten werden als Datamatrixcode auf Papier ausgedruckt und dem Patienten als Beiblatt mit der Rechnung per Post übersandt oder persönlich übergeben. Der dazugehörige Einmalschlüssel wird über den PKV-Pseudodatenpool übermittelt.

6.2.2. Clientsysteme

Bei den begutachteten Komponenten der Clientsysteme handelt es sich um die in der Abbildung 2a mit Client 1 und Client 2 bezeichneten Komponenten, die sowohl auf der Seite des Rechnungserstellers als auf der Seite der Zahlstelle vorhanden sind. Die Clientsysteme sind auf der Seite des Rechnungserstellers und der Seite der Zahlstelle grundsätzlich gleichartig aufgebaut und werden in die vorhandene Umgebung des Rechnungserstellers bzw. des Leistungsträgers integriert (vgl. Abbildungen 3 und 4). Jedes Clientsystem besteht aus Client 1 und Client 2. Client 1 dient auf beiden Seiten zum Datenaustausch mit dem Pseudodatenpool. Client 2 dient insbesondere der Ver- bzw. Entschlüsselung der auf dem Beiblatt übermittelten Rechnungsdaten und der versandfertigen Erstellung der Beiblätter als solches.

Im Kernsystem des Rechnungserstellers (in der Abb. 2b mit U2/Kernsystem bezeichnet) wird die Rechnung erstellt. Der Client2 auf der Rechnungserstellerseite (U2/Client2) bereitet die Rechnung entsprechend der Vorgaben des Pseudodatenpools auf, erzeugt den Einmalschlüssel und verschlüsselt die Beiblattdaten mit diesem. Der Einmalschlüssel wird mit der entsprechenden Referenznummer an das Modul zum Datenaustausch mit dem Pool (U1/Poolzugriff) übergeben. Der Client1 des Rechnungserstellers (U1/Client1) dient der Weitergabe des Einmalschlüssels und der Referenznummer an den Pseudodatenpool. Das Modul zum Rechnungsversand (U3/Rechnungsversand) erstellt neben der eigentlichen Rechnung auch das Beiblatt zum Versand an den Versicherungsnehmer.

Auf der Seite des Leistungserbringer erfolgt der Eingang der Rechnung und sofern vom Versicherungsnehmer übermittelt des Beiblatts im Modul U3'/Empfang. Nach Eingang eines Beiblatts wird im Modul des Kernsystems auf der Seite des Leistungserbringers (U2'/Kernsystem) das Beiblatt eingescannt und digitalisiert. Um die Daten des Beiblatts rekonstruieren zu können benötigt U2' Kernsystem den Einmalschlüssel aus dem Pseudodatenpool. Diese Anforderung wird an das Modul zum Poolzugriff (U1'/Poolzugriff) übergeben. Über den Client1 (U1'/Client1) wird auf den Pseudodatenpool zugegriffen um den Einmalschlüssel abzurufen. Dieser wird an U2'/Kernsystem übergeben. Nach der Entschlüsselung im U2'/Client2 werden die Beiblattdaten rekonstruiert und fließen in den Prozess zur Abrechnung ein.

6.3. Funktionale Beschreibung

Bisher erfolgt der Rechnungsdatenaustausch im Bereich der privaten Krankenversicherungen (PKV) und der Beihilfestellen papierbasiert. Der Patient erhält von seinem Arzt eine ausgedruckte Rechung. Diese Rechnung wird vom Patienten bei seiner PKV bzw. Beihilfestelle eingereicht. Dort werden die Daten der Rechnungen erfasst und automatisiert verarbeitet.

Die Idee des PKV-Pseudodatenpool ist, zum einen den Medienbruch bei der Weitergabe der Rechnung zu vermeiden und zum anderen sicherzustellen, dass Übermittlung der Rechnungsdaten genauso sicher bleibt wie bisher. Hierzu werden im Clientsystem des Rechnungserstellers die Rechnungsdaten mit einem per Zufallszahlengenerators erzeugten Einmalschlüssel verschlüsselt und zusätzlich zur Rechnung die verschlüsselten Rechnungsdaten als Datamatrixcode auf ein Beiblatt ausgedruckt. Ergänzend wird auf dem Beiblatt die Schlüsselreferenz für diesen Einmalschlüssel ausgedruckt Der Patient erhält nun die Rechnung und auch das Beiblatt zur Rechnung. Das Clientsystem des Leistungserbringers übermittelt nun auf einem gesicherten Weg den Schlüssel mitsamt der Schlüsselreferenz an den PKV-Pseudodatenpool (vgl. Abbildung 3). Der Schlüssel und auch die Schlüsselreferenz lassen keinerlei Rückschlüsse auf den Patienten oder die Rechnungsdaten zu. Nur der Leistungserbringer kann über die Schlüsselreferenz identifiziert werden.

Wie bisher reicht der Patient die Rechnung beim Leistungsträger (also PKV- oder Beihilfestelle) ein (vgl. Abbildung 4 Schritt 2). Dieser Schritt 2 ist nur der Vollständigkeit halber dargestellt. Die freiwillige Weitergabe des Beiblatts des Patienten an die Zahlstelle ist zwar eine wesentliche Vorraussetzung dafür damit die Zahlstelle den Einmalschlüssel zu diesem Beiblatt aus dem Pseudodatenpool abrufen kann um damit die Rechnungsdetails aus dem eingereichten Beiblatts zu rekonstruieren. Der Vorgang selbst kann allerdings nicht Bestandteil der Begutachtung und Zertifizierung sein.

Wenn der Patient nun nicht nur die Rechnung sondern auch das Beiblatt (oder auch nur das Beiblatt) bei dem Leistungsträger einreicht, kann das Clientsystem des Leistungsträgers über die aufgedruckte Schlüsselreferenz auf gesicherten Weg den Einmalschlüssel zur Entschlüsselung der Rechnungsdaten aus dem PKV-

Pseudodatenpool abrufen und damit die – als Datamatrixcode erhaltenen – verschlüsselten Rechnungsdaten entschlüsseln (vgl. Abbildung 5).

Durch die Nutzung des PKV-Pseudodatenpool erfolgen – abgesehen von der Abrechung der Nutzung des PKV-Pseudodatenpools – keine zusätzlichen Datenverarbeitungen oder Nutzungen. Die Verarbeitung der Daten zur Abrechung der Nutzung des PKV-Pseudodatenpools erfolgt auf freiwilliger vertraglicher Grundlage. Einer Beihilfestelle oder PKV entstehen bei der Nichtnutzung des PKV-Pseudodatenpools keine Nachteile gegenüber dem bisherigen Verfahren.

Bei entsprechender Ausgestaltung der Verträge zwischen Versicherten und PKV wäre es auch ausreichend, wenn der/die Versicherte nur das Beiblatt beim Leistungsträger einreicht. Eine entsprechende Organisation des Leistungsträgers vorausgesetzt, könnte hierdurch sichergestellt werden, dass nur die Mitarbeiter/innen Zugriff auf die Rechnungsdaten erhalten, die diesen für ihre Tätigkeit benötigen. Dies würde die Vertraulichkeit der Rechnungsdaten auch innerhalb der Leistungsträger erhöhen.

6.4. Zweck und Einsatzbereich

Sichere Übermittlung der Rechnungsdaten von Leistungserbringen zu Leistungsträgern im Bereich der Abrechnung zwischen Leistungserbringern und privaten Krankenversicherungen sowie Beihilfestellen.

6.5. Modellierung des Datenflusses

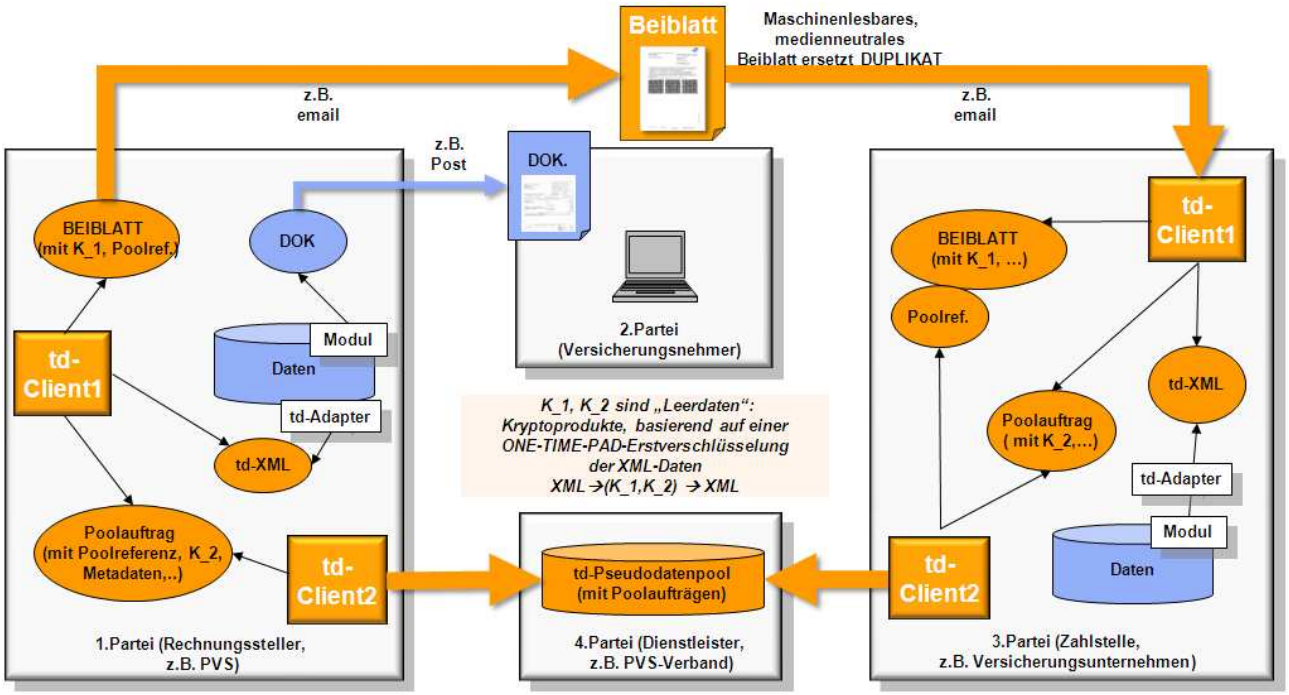

Abbildung 1: Schematische Übersicht

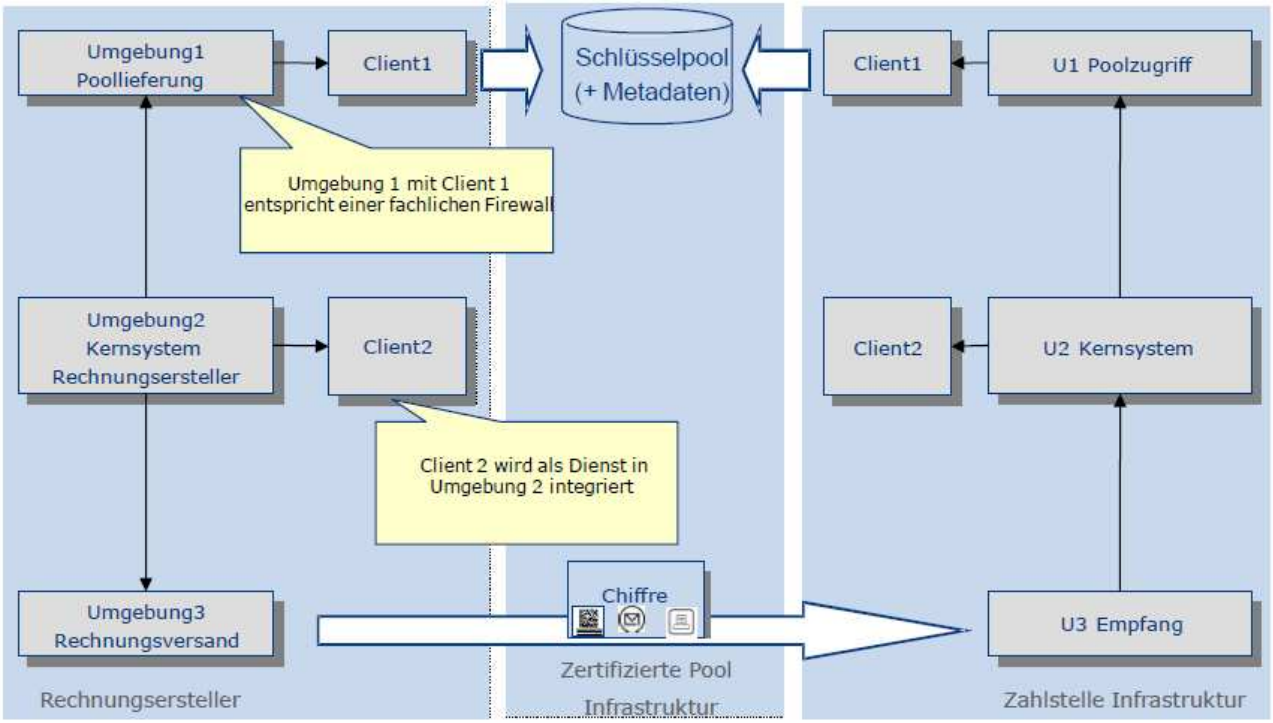

Abbildung 2a: Darstellung der Clientsystem auf Sender- und Abruferseite

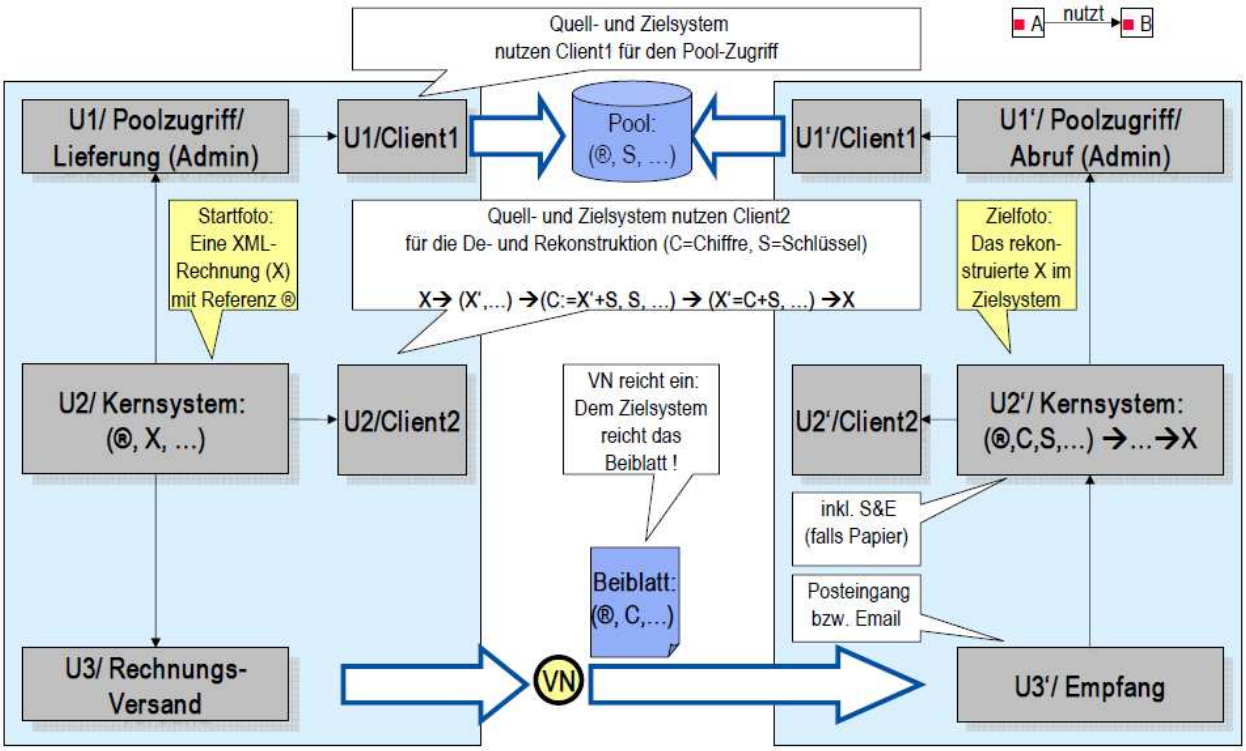

Abbildung 2b: Funktionale Darstellung der Clientsysteme

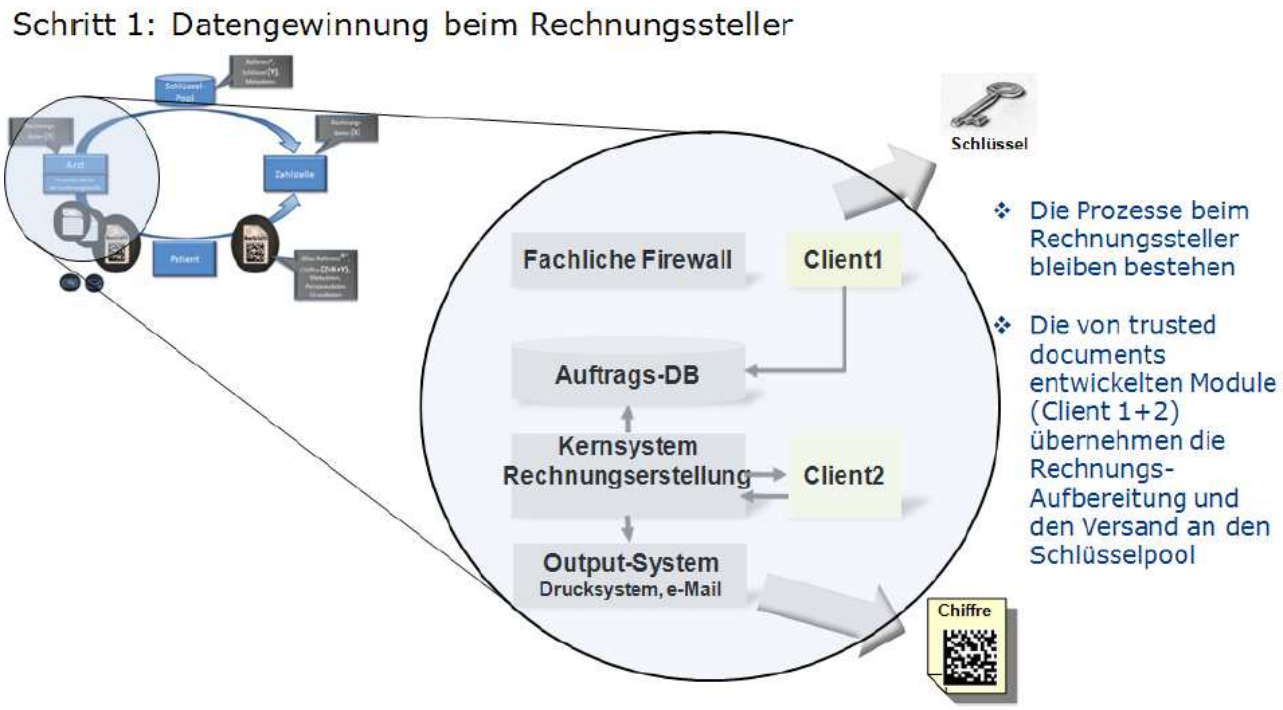

Abbildung 3: Darstellung Schritt 1 Datengewinnung beim Rechnungssteller

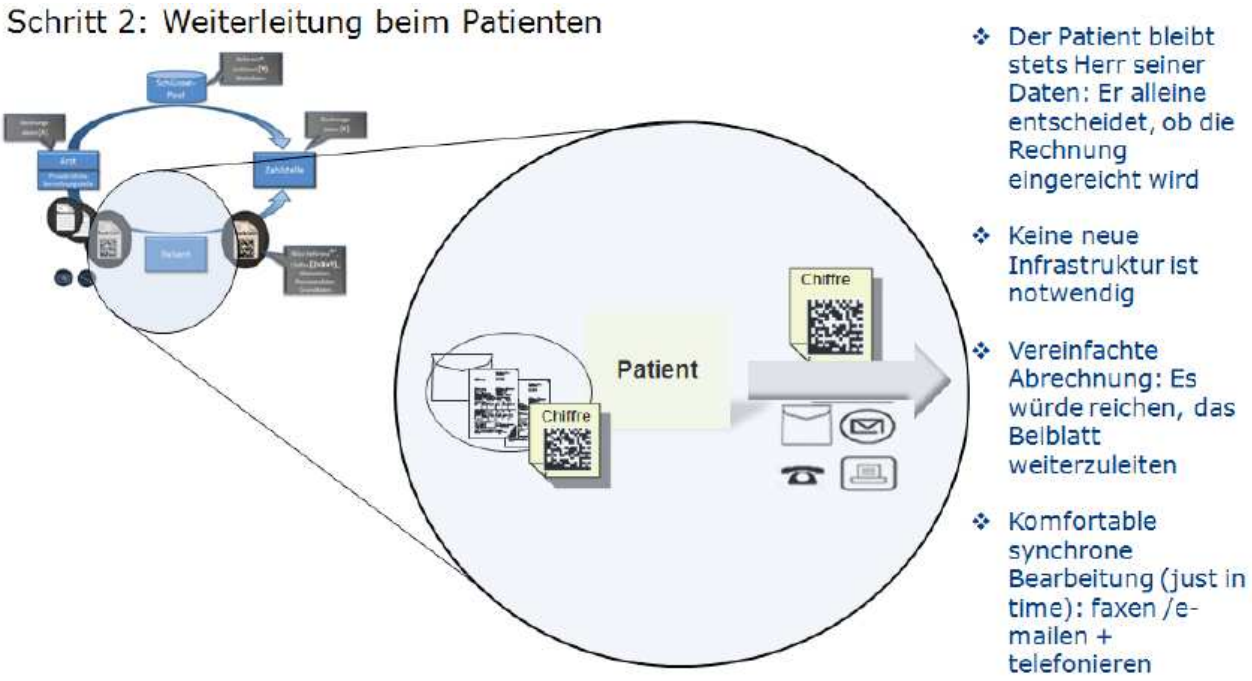

Abbildung 4: Darstellung Schritt 2 Weiterleitung beim Patienten

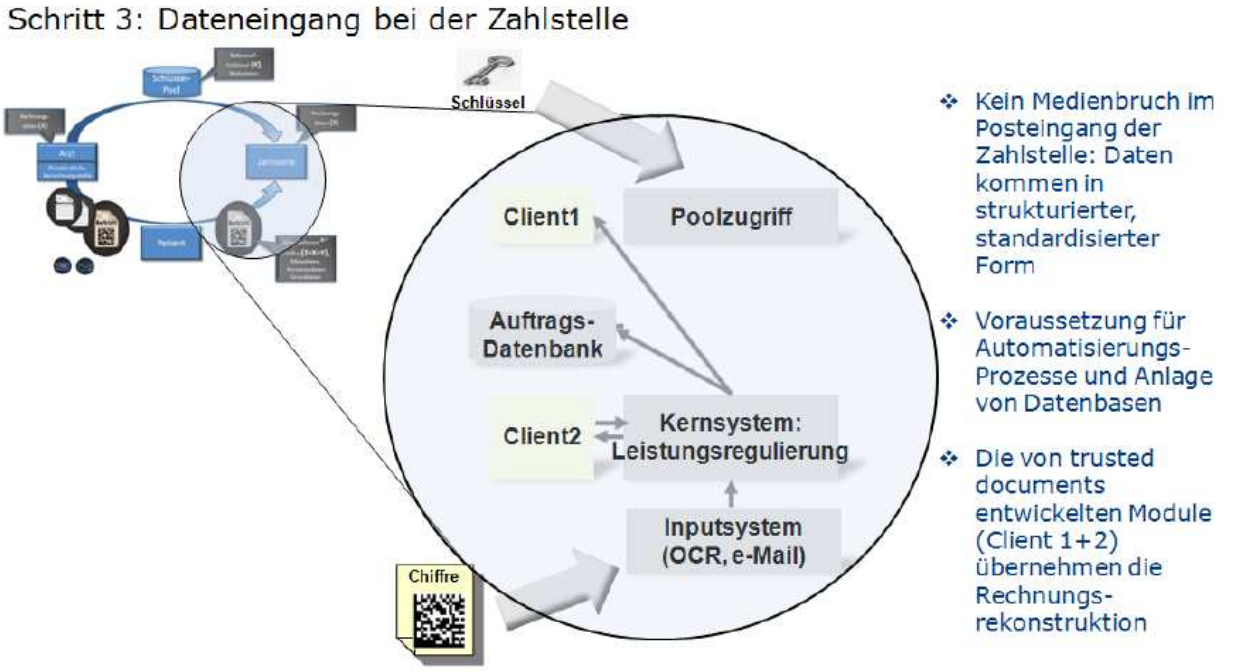

Abbildung 5: Darstellung Schritt 3 Dateneingang bei der Zahlstelle

7. Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Anforderungskatalog v 1.2 vom 29.08.2005

8. Zusammenfassung der Prüfungsergebnisse

Die Aussagen für den Pseudodatenpool aus dem Kurzgutachten vom Juni 2008 gelten weiterhin. Zu der Bewertung der Clientsysteme vgl. Abschnitt 8.1.2

8.1. Besonderheiten

Das Verfahren zeichnet sich durch zwei Besonderheiten aus: Zum einen wird als Datenträger für die dezentrale Übermittlung der automatisiert verarbeitbaren Daten Papier verwendet (optional e-Mail), zum anderen wird das als absolut sicher geltende Onetimepad-Verschlüsselungsverfahren für die Erstverschlüsselung angewendet. Das Ergebnis dieser beiden Besonderheiten ist der Umstand, dass im PKV-Pseudodatenpool keine Rechnungsdaten gespeichert werden, sondern nur die Einmalschlüssel, die erforderlich sind, um die Daten, die auf dem Beiblatt verschlüsselt als Datamatrixcode aufgedruckt wurden, zu entschlüsseln. Da das Beiblatt mit der Rechnung an den Versicherten bzw. Beihilfeberechtigten übermittelt wird (persönlich oder per Post), ergibt sich durch den Ausdruck der verschlüsselten Rechnungsdaten sowie einer Referenz auf den Einmalschlüssel in maschinenlesbarer Form kein zusätzliches Risiko bei der Übermittlung. Die Abspeicherung der zu den verschlüsselten Rechnungsdaten gehörenden Einmalschlüssel stellt auch kein zusätzliches Risiko bei der Übermittlung dar, da die Einmalschlüssel keinerlei Bezug zum Versicherte bzw. Beihilfeberechtigten haben. Einzig der Leistungserbringer bzw. dessen Abrechnungsdienstleister (Portal oder PVS) lassen sich aus der Schlüsselreferenz ableiten.

8.1.1. Beiblatt mit Datamatrixcode

Die Aussagen zum Beiblatt aus dem Gutachten vom Juni 2008 gelten unverändert.

8.1.2. Onetimepad-Verschlüsselungsverfahren

Wesentlicher Aspekt für die Sicherheit des Onetimepad-Verschlüsselungsverfahren ist eine Erzeugung von Pseudozufallszahlen, die von einer echten zufälligen Erzeugung möglichst wenig abweicht. Mit dem eingesetzten Verfahren gelingt es dem Hersteller, Pseudozufallszahlen in ausreichender Länge von sehr guter Qualität zu erzeugen. Dadurch ist eine wirksame Verschlüsselung der Rechnungsdaten im Datamatrixcode auf dem Beiblatt gewährleistet.

8.2. Rahmenvertrag

Die Aussagen zum Rahmenvertrag aus dem Gutachten vom Juni 2008 gelten unverändert.

9. Beschreibung, wie das IT-Produkt den Datenschutz fördert

Die Aussagen aus dem Gutachten vom Juni 2008 für den Pseudodatenpool gelten unverändert.

Durch die Einbeziehung der Clientsysteme in die Zertifizierung wird seitens des Herstellers nun sichergestellt, dass Clientsysteme zum Einsatz kommen, die die sicherheitstechnischen Anforderungen des Herstellers aus dem Rahmenvertrag erfüllen. Somit ist eine sichere Einmal-Verschlüsselung der Rechnungsdaten nicht nur gefordert, sondern durch den Einsatz der Clientsysteme auch gewährleistet.

9.1. Rechnungsversand per E-Mail

Grundsätzlich bietet dieses System auch die Grundlage für einen sicheren Versands der Beiblätter per E-Mail als Duplikat-Ersatz der Rechnung, sofern dies vom Versicherungsnehmer gewünscht ist. Für diese Nutzung ist eine sichere Kommunikation zwischen Rechnungsersteller und Versicherungsnehmer erforderlich. Die Inhaltsdaten können über eine sichere asymmetrische Verschlüsselung vor unbefugten Zugriff geschützt werden. Hier stellt sich allerdings das Problem, dass alleine die Tatsache, dass zwischen einem Arzt und einem Patienten Daten ausgetauscht werden zumindest bei Inanspruchnahme von Fachärzten Rückschlüsse auf den Gesundheitszustand oder bestimmte Erkrankungen schließen lassen. Eine Lösung bietet auch hier ein „Hausarzt-Modell“. Sofern der Versicherungsnehmer es wünscht werden die Rechnungsdaten dann nicht direkt sondern über den Umweg des Hausarztes versandt:

Der Leistungserbringer bzw. Rechnungsersteller sendet auf Wunsch des Versicherungsnehmers das mit dem Pulic-Key des Versicherungsnehmers verschlüsselte Beiblatt sowie die E-Mail-Adresse des Versicherungsnehmers mittels einer mit dem Public-Key des Hausarztes verschlüsselten E-Mail an den Hausarzt des Versicherungsnehmers. Das Praxissystem des Hausarztes entschlüsselt diese E-Mail und leitet das immer noch mit dem Public-Key des Versicherungsnehmers verschlüsselte Bei-

blatt an die angegebene E-Mail-Adresse des Versicherungsnehmers weiter, sofern diese dem Hausarzt (bzw. seinem Praxissystem bekannt ist). Der Hausarzt erfährt zwar auf diesem Weg die Absendeadresse der Rechnung, aber keine Rechnungs- oder gar Behandlungsdaten. Nur wenn die Rechnung direkt von einem Leistungserbringer erstellt wird, lässt sie grobe Rückschlüsse auf die Fachrichtung des Arztes oder die Art der Leistungserbringung zu. Durch entsprechende Anpassung des Praxissystems kann der Kontaktschutz weitgehend automatisiert abgewickelt werden. Der Hausarzt hätte somit (fast) keinen Mehraufwand.

Der Versicherungsnehmer selbst entschlüsselt nun das Beiblatt und kann es nun mit dem entsprechenden Public-Key des Leistungsträgers verschlüsselt an diesen versenden. Da für die Zahlungsabwicklung das Beiblatt ausreichend ist, wäre bei entsprechender vertraglicher (oder gesetzlicher) Gestaltung der Abrechnungsgrundlagen die Einreichung der Rechnung in Papierform nicht mehr erforderlich. Durch entsprechende technische und organisatorische Maßnahmen auf Seiten der Leistungsträger würde sich so sicherstellen lassen, dass nur die Mitarbeiter/innen des Leistungsträgers auf abrechungsrelevante Gesundheitsdaten zugreifen können, die dies zu Abrechnungszwecken benötigen.