Kurzgutachten

PKV-Pseudodatenpool V 1.0 der trusted documents GmbH

1. Zeitpunkt der Prüfung

Dezember 2007 bis Juni 2008

2. Adresse des Antragstellers

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

3. 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

4. Kurzbezeichnung des IT-Produktes

PKV-Pseudodaten-Pool –- bürgerfreundlicher (PKV-)Rechnungsdatenaustauch (brda) -, (basierend auf einer Erfindung von Robert Niggl, die unter dem Aktenzeichen 10 2008 014 187.9-53 beim Deutschen Patent- und Markenamt eingereicht wurde). Prüfungsgegenstand ist der PKV-Pseudodatenpool V 1.0 mit seinen Schnittstellen und der Rahmenvertrag zwischen dem Betreiber und seinen Vertragspartnern.

5. Detaillierte Bezeichnung des IT-Produktes

Gegenstand der Zertifizierung ist der PKV-Pseudodaten-Pool - bürgerfreundlicher (PKV-)Rechnungsdatenaustauch (brda) -, (basierend auf einer Erfindung von Robert Niggl). Prüfungsgegenstand ist der PKV-Pseudodatenpool V 1.0 mit seinen Schnittstellen und der Rahmenvertrag zwischen dem Betreiber und seinen Vertragspartnern. Die Clients, die zur Nutzung des Pools verwendet werden, sind nicht Gegenstand der Begutachtung.

5.1. 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). 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.

5.2. Technische Beschreibung

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. Die Datenübermittlung durch Rechnungssteller 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 Verschlüsselung der Rechnungsdaten selbst erfolgt mit dem Onetimepad-Verfahren unter Verwendung der XOR (Exklusive ODER)-Verschlüsselung. Bei dem eingesetzen Ontimepad-Verfahren wird im Clientsystem des Leistungserbringers 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.

5.3. 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 Zufallszahlengenerator 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 die Rechnung und auch das Beiblatt zur Rechnung. Das Clientsystem des Rechnungserstellers übermittelt nun auf einem gesicherten Weg den Schlüssel mitsamt der Schlüsselreferenz an den PKV-Pseudodatenpool. 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. 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 Leistungserbringers über die aufgedruckte Schlüsselreferenz auf gesichertem Weg den Einmalschlüssel zur Entschlüsselung der Rechnungsdaten aus dem PKV-Pseudodatenpool abrufen und damit die – als Datamatrixcode erhaltenen – verschlüsselten Rechnungsdaten entschlüsseln.

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.

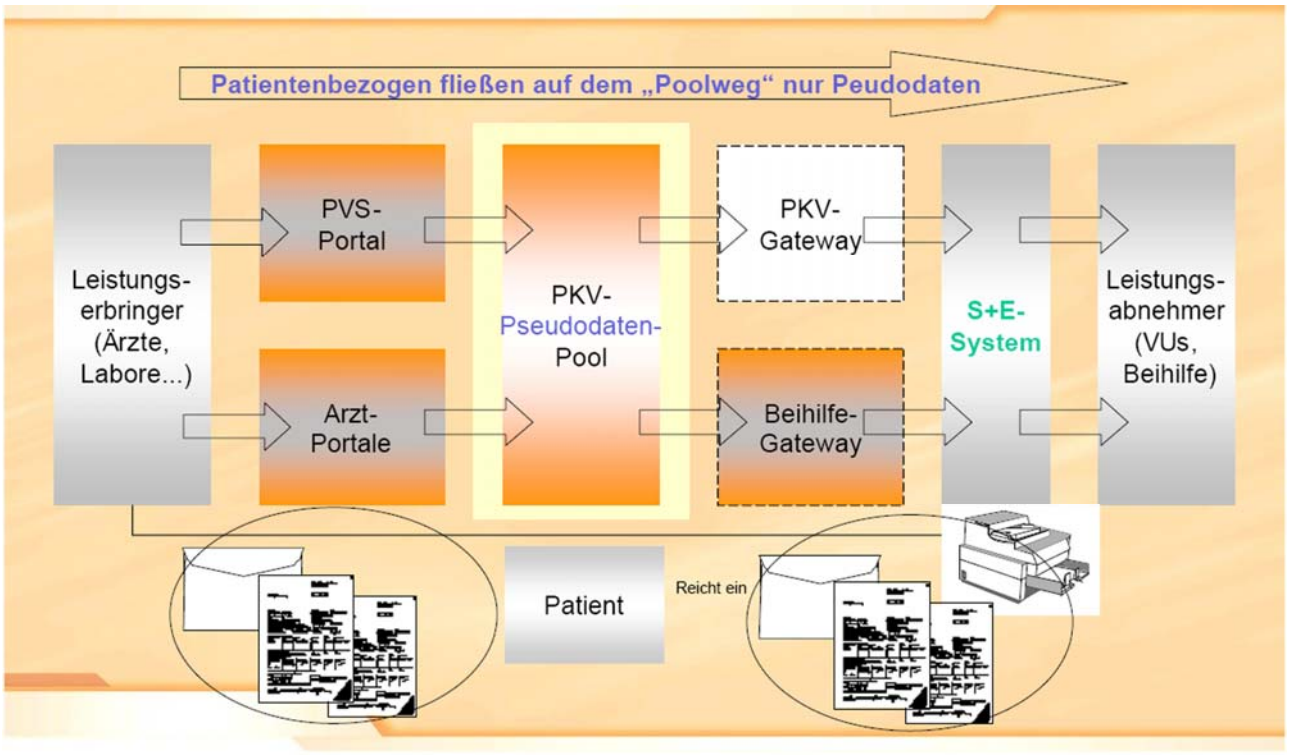
Bei entsprechender Ausgestaltung der Verträge zwischen Versicherten und PKV wäre es auch ausreichend, wenn der/die Versicherte nur das Beiblatt beim Leistungsträger einreicht. Eine entsprechende Organisation des Leistungsträgers vorausgesetzt, könnte hierdurch sichergestellt werden, dass nur die Mitarbeiter/innen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

Dies würde die Vertraulichkeit der Rechnungsdaten auch innerhalb der Leistungsträger erhöhen.

5.4. Zweck und Einsatzbereich

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

5.5. Modellierung des Datenflusses



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

Anforderungskatalog v 1.2 vom 29.08.2005

7. Zusammenfassung der Prüfungsergebnisse

Der PKV-Pseudodatenpool ist ein Beispiel für eine vorbildliche Umsetzung der Vorschriften über den Datenschutz und die Datensicherheit im Umfeld medizinischer Rechnungsdaten. Es ermöglicht die automatisierte Weiterbearbeitung dieser sensiblen Rechnungsdaten der Leistungserbringer bei den Leistungsträgern, ohne dass die Übertragung der Rechnungsdaten von den Leistungserbringern zu den Leistungsträgern wirksame Angriffe auf die Vertraulichkeit der Rechnungsdaten zu lie-

ße. Daher kommt dieses Verfahren dem Wunsch vieler Leistungsträger entgegen, den Medienbruch zwischen Rechnungsausdruck bei Leistungserbringer oder dessen Dienstleister und dem Erfassen der Rechnungsdaten beim Leistungsträger zu vermeiden ohne zusätzliche Risiken beim Datenschutz und der Datensicherheit mit sich zu bringen.

Die Rechnungsdaten werden – wie bisher – vom Leistungserbringer dem Versicherten bzw. Beihilfeberechtigten übergeben oder per Post übersandt. Der Versicherte bzw. Beihilfeberechtigte entscheidet selbst, ob er die Rechnung zur Abrechnung mit der PKV bzw. der Beihilfestelle einreicht (persönlich oder per Post) oder auf eine Abrechnung verzichtet und die Rechnung selbst bezahlt. Bei der Einreichung kann der Versicherte bzw. Beihilfeberechtigte entscheiden, ob er das Beiblatt mit den verschlüsselten Rechnungsdaten beim Leistungsträger einreicht. Nur mit diesem Beiblatt – und dem darauf referenzierten Einmalschlüssel aus dem PKV-Pseudodatenpool – ist es dem Leistungserbringer möglich, die Rechnungsdaten automatisiert zu erfassen. Da der Weg der Rechnungsdaten gegenüber dem bisherigen Verfahren nicht verändert wird und im PKV-Pseudodatenpool nur die zu den jeweiligen Rechnungen gehörenden Einmalschlüssel abgelegt werden, werden durch das Verfahren PKV-Pseudodatenpool die bisherigen Datenübermittlungen nicht erweitert. Die einzige Änderung der Datenverarbeitung im Rahmen der Abrechung der Leistungserbringer ergibt sich – sofern der Versicherte oder Behilfeberechtigte das Beiblatt zur Rechnung bei dem Leistungsträger einreicht – aus der Möglichkeit auf die manuelle Erfassung zu verzichten und die im Datamatrixcode übermittelten verschlüsselten Rechnungsdaten einzulesen und mit den Einmalschlüssel aus dem Datenpool zu entschlüsseln. Der Kreis der Personen, die Zugriff auf die Rechnungsdaten hat, wird dadurch nicht erweitert, sondern kann sogar reduziert werden.

7.1. Besonderheiten

Das Verfahren zeichnet sich durch zwei Besonderheiten aus: Zum einen wird als Datenträger für die Übermittlung der automatisiert verarbeitbaren Daten Papier verwendet, zum anderen wird das als sehr sicher geltende Ontimepad-Verschlüsselungsverfahren angewendet. Das Ergebnis dieser beiden Besonderhei-

ten 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.

7.2. Rahmenvertrag

Im Rahmenvertrag sind wesentliche clientseitige Anforderungen geregelt. Dabei ist es grundsätzlich möglich, dass es mehrere PKV-Pseudodatenpool-Betreiber gibt. Dieses Gutachten gilt nur für PKV-Pseudodatenpoolbetreiber, die den als Anlage zum Gutachten beigefügten Rahmenvertrag sowie die damit verbundene Anlage zur Partnerzertifizierung verwenden.

Neben dem Poolbetreiber können Leistungserbringer bzw. deren Abrechnungsdienstleister (im Vertrag Lieferanten genannt) und Leistungsträger (PKV, Beihilfestellen bzw. deren Abrechnungsdienstleiser, im Vertrag Abrufer genannt) Vertragspartner werden. Nur Vertragspartner können am Verfahren des PKV-Pseudodatenpools teilnehmen. Um Vertragspartner werden zu können, ist es erforderlich, dass sowohl Lieferanten als auch Abrufer durch einen unabhängigen Prüfer gemäß der Anlage Partnerzertifizierung zum Rahmenvertrag zertifiziert wurden. Bei der Zertifizierung ist insbesondere zu prüfen, ob die Installation der für die Verschlüsselung erforderlichen Komponenten vertragskonform erfolgte.

Durch den Rahmenvertrag zum Betrieb des PKV-Pseudodatenpool verpflichtet sich der Lieferant dazu,

- für die Datenübertragung zum PKV-Pseudodatenpool nur die freigegebenen Softwaremodule zu verwenden und nachträgliche Änderungen unverzüglich und schriftlich dem Poolbetreiber zu melden.
- zu jeder PKV-relevanten Rechnung einen Datensatz im vorgegebenen Format zu erzeugen. Der erzeugten Rechnungsdatensatz ist dann über das Clientsystem zu verschlüsseln und als Datamatrixcode auf einem Beiblatt zur Rechnung an den Patienten zu übergeben. Der für die Verschlüsselung erzeugte Einmalschlüssel ist über das Clientsystem in den Datenpool einzustellen.

Im Rahmenvertrag sind Sanktionen bei Verstößen gegen Regelungen des Rahmenvertrags festgelegt. Bei Einhaltung dieser Regelungen ist sichergestellt, dass weder versehentlich unverschlüsselte Rechnungsdaten als Datamatrixcode auf das Beiblatt zur Rechung gedruckt werden noch dass statt des Einmalschlüssels die verschlüsselten oder gar unverschlüsselten Rechnungsdaten in den Datenpool eingestellt werden.

Sofern der PKV-Pseudodatenpool anderen Betreibern zur Verfügung gestellt wird, ist seitens der trusted documents GmbH als Hersteller des PKV-Pseudodatenpools sicherzustellen, dass überprüft werden kann, dass ein Poolbetreiber, der damit wirbt, ein mit dem Datenschutzgütesiegel versehendes Produkt zu verwenden, zumindest die für die Sicherstellung der Funktionalität des Verschlüsselungsverfahrens erforderlichen Vertragsbestimmungen aus dem Rahmenvertrag unverändert mit seinen Vertragspartnern vereinbart hat.

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

Der Datenschutz wird durch PKV-Pseudodatenpool insbesondere dadurch gefördert, dass die automatisiert verarbeitbaren Rechnungsdaten zwischen Leistungserbringer und Leistungsträger nur in verschlüsselter Form übertragen werden und der/die betroffene Patient/in selbst entscheiden kann, ob er/sie diese automatisiert verarbeitbaren Daten dem Leistungsträger übermittelt oder diesem nur die Rechnung in Papierform übergibt.

Das Verfahren ermöglicht auch auf die Einreichung der Klartextrechnung zu verzichten und nur das Beiblatt mit den verschlüsselten Rechnungsdaten für die Ein-

reichung beim Leistungsträger zu nutzen. In diesem Fall würde der Posteingang der Leistungsträger keinen Zugriff auf die Rechnungsdaten haben. So könnte sichergestellt werden, dass nur die Mitarbeiter/innen des Leistungsträgers, die den Zugriff auf die Rechnungsdaten für ihre Tätigkeit benötigen, diesen auch erhalten.

Das eingesetzte One-Time-Pad-Verfahren zur Verschlüsselung wird in dieser Form der Schlüsselübertragung erstmalig verwendet und stellt in dieser Kombination eine praktikable Form des als sehr sicher bezeichneten OTP-Verfahrens.

Zur Sicherstellung der Eingabekontrolle erfolgt eine Protokollierung der Aktivitäten der Mitarbeiter des Betreibers des PKV-Pseudodatenpools. Die Auswertungen der Mitarbeiteraktivitäten erfolgen grundsätzlich ohne Bezug zum/zur Mitarbeiter/in. Nur der Benutzer mit der Rolle REVISOR kann auch benutzerbezogene Sonderauswertungen anstoßen. Diese sind vom System mit dem Schlüssel einer weiteren Person, beispielsweise des/der Datenschutzbeauftragten verschlüsselt, so dass der Zugriff auf diese benutzerbezogenen Sonderauswertungen mit dem Vieraugenprinzip geschützt ist. Der Nutzer mit der Rolle Datenschutzbeauftragter kann die vom Nutzer mit der Rolle Revisor angestoßenen Sonderauswertungen entweder freigeben oder ablehnen. Die Auswertungen stehen dem Revisor nach der Freigabe max. 14 Tage zur Verfügung.