

Langzeitsignaturen für elektronische Patientenakten und andere medizinische Dokumente

Langzeitsignaturen für elektronische Patientenakten und andere medizinische Dokumente

Michael Herfert, Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Darmstadt

Handschriftlich geleistete Signaturen unterliegen einem Alterungsprozess. Digitale Signaturen können zwar nicht verblassen, doch auch sie altern und verlieren dadurch an Wert. Dieser Wertverlust wird schon nach sechs Jahren signifikant. Alle Anwender, die Signaturen auch danach noch beweissicher verifizieren wollen, müssen rechtzeitig und regelmäßig Gegenmaßnahmen ergreifen. Als Anwender sind insbesondere Ärzte, Zahnärzte, Apotheker und andere Heilberufler zu sehen, denn diese Gruppen werden den Heilberufsausweis erhalten, der eine digitale Signatur nach Signaturgesetz ermöglicht.

Dieses Papier erläutert aus technischer Sicht die Hintergründe des Alterns digitaler Signaturen und zeigt, wie sie dennoch über Jahrzehnte in ihrem Wert erhalten werden können. Das dabei eingesetzte Verfahren eignet sich gleichzeitig zum Nachweis der Integrität unsignierter Dokumente im Sinne der Revisionsicherheit. Im Gegensatz zu etablierten Lösungen, die auf WORM-Speichern oder anderer Hardware beruhen, kann das hier vorgestellte Prinzip allein in Software realisiert werden.

1 Prolog 2020

November 2020. Katharina S. leidet seit Jahren an den Folgen einer Asbestvergiftung. Ihr Zustand ist bedauerlich und einen großen Anteil daran trägt das Krankenhaus, so Katharina S. Sie wirft den behandelnden Ärzten vor, ihre Krankheit viel zu spät erkannt zu haben. Schon 2008 hätte das Krankenhaus ihre Symptome erkennen und eine Behandlung einleiten müssen. Im Angesicht ihres schlimmen Zustands verklagt Katharina S. das Krankenhaus auf Schmerzensgeld. Das Krankenhaus seinerseits bestreitet jeglichen Fehler. Es sieht dem Prozess mit Gelassenheit entgegen, schließlich gehörte Katharina S. im Jahr 2008 zu den ersten Patienten, deren Akten rein digital geführt wurden. Jeder Eintrag in ihrer Akte wurde durch einen Arzt digital signiert. Dazu verwendeten die Ärzte den Heilberufsausweis, der wenige Jahre zuvor eingeführt worden war. Mit Hilfe dieser Smartcard leisteten die Ärzte digitale Signaturen nach den strengen Richtlinien des deutschen Signaturgesetzes. Um diese Richtlinien umzusetzen, hatten Ärzte, Zahnärzte, Apotheker, Krankenhaus, das Bundesgesundheitsministerium und andere Beteiligte seinerzeit viel Zeit und Geld investiert. Da das deutsche Signaturgesetz als das Strengste der Welt gilt, sieht das Krankenhaus es als gegeben an, Integrität und Authentizität der gesamten Patientenakte vor Gericht beweisen zu können.

Das Krankenhaus legt dem Richter die Patientenakte vor, aus der kein Hinweis auf eine Asbestvergiftung zu entnehmen ist. Aus den Aufzeichnungen des Trustcenters geht hervor, dass die damals beteiligten Ärzte ihre Chipkarten bei einem turnusmäßigen Schlüsselwechsel abgegeben hätten, daher sei eine nachträgliche Verfälschung auszuschließen, so das Krankenhaus. Der Richter überprüft mit seinem Rechner alle digitalen Signaturen und stellt ihre Korrektheit fest. Dem Anwalt von Katharina S. wird ebenfalls die Akte vorgelegt. Auch er kann keinen Fehler finden. Er bemerkt aber, dass alle Signaturen mit einer Schlüssellänge von 2048 Bits geleistet wurden. Er wendet ein, dass diese Schlüssellänge zwar im Jahre 2008 als sicher gegolten habe, dass heute, also 12 Jahre später, eine derartige Signatur von jedem Taschencomputer gebrochen werden könne. Der Anwalt merkt an, dass das Krankenhaus keinerlei Maßnahmen getroffen habe, die Signatur zu erhalten, sie also vor dem kryptographischen „Verblässen“ zu schützen, daher könne die Integrität des Dokuments nicht mehr kryptographisch bewiesen werden. Vielmehr sei es überhaupt nicht auszuschließen, dass das Krankenhaus belastende Teile der Patientenakte entfernt habe. Dazu seien nicht einmal die alten Chipkarten erforderlich, denn das Krankenhaus selbst sei heute in der Lage, damalige Signaturen zu fälschen. Das Krankenhaus bestreitet vehement jegliche Manipulation der Akte. Der Richter zieht einen Gutachter hinzu, um den Sachverhalt zu untersuchen. Dieser stellt fest, dass die Signaturen tatsächlich ihren kryptographischen Beweiswert verloren haben. Der Richter schließt daraufhin die Signatur als Beweismittel aus. Er merkt an, dass das Krankenhaus seiner Pflicht zur Beweiserhaltung digitaler Signaturen nicht nachgekommen sei, daher könne nun die Entscheidung nicht mehr durch die Verifikation einer digitalen Signatur getroffen werden, was sehr einfach gewesen wäre, sondern es müssten die vielfältigen Argumente beider Parteien abgewogen werden, um zu einer Entscheidung zu kommen. Der Ausgang des Verfahrens ist offen.

2 Archivierung digitaler Dokumente

Zurück im Jahr 2006.

Mit der Einführung der neuen Telematikinfrastruktur für das Gesundheitswesen wird es zu einer Vielzahl digital signierter Dokumente kommen. Zunächst werden elektronische Rezepte digital signiert werden, da diese Anwendung im GMG vorgeschrieben wird. Später werden weitere Anwendungen hinzukommen, zu groß ist der Rationalisierungseffekt, der sich aus einer elektronischen Dokumentenverarbeitung ohne Medienbruch ergibt. Schon heute existieren Vorschläge, wie elektronische Patientenakten strukturiert sein könnten und wie sie digital zu signieren sind. Der elektronische Arztbrief ist eine weitere Anwendung, für die es heute schon Implementierungen gibt, welche eine digitale Signatur berücksichtigen.

Der Gesetzgeber schreibt je nach Art des Dokuments sehr lange Aufbewahrungsfristen vor. Sie reichen von 10 Jahren (§10 Abs. 3 Musterberufungsverordnung für Ärzte [RoÄ]) bis hin zu 30 Jahren (z.B. §28 Abs. 3 Röntgenverordnung [RoÄ]). Aufbewahrungsfristen von mehreren Jahrzehnten sind also nicht ungewöhnlich. Bei Papierbasierten Dokumenten ist das Problem schon seit vielen Jahren bekannt. So benutzt man dokumentenechte Tinte, damit Unterschriften nicht verblassen, und man bewahrt wichtige Dokumente in einer Umgebung auf, die das richtige Maß an Luftfeuchtigkeit besitzt und vor direkter Sonneneinstrahlung geschützt ist. All das ist bekannt und wird im Gesundheitswesen, im Verwaltungsbereich, im Steuerwesen, im Bankenbereich und anderen Anwendungsfällen, bei denen der Gesetzgeber Aufbewahrungsfristen vorschreibt, seit langem erfolgreich praktiziert.

Im Bereich der elektronischen Langzeitarchivierung sind die Probleme neuer, die Lösungen, soweit sie überhaupt praktiziert werden, noch weitaus weniger etabliert. Von einem prinzipiellen Standpunkt aus lassen sich drei Problembereiche identifizieren: ...

Dokumentinformationen zum Volltext-Download

Ä

Titel:

Langzeitsignaturen für elektronische Patientenakten und andere medizinische Dokumente Artikel ist erschienen in: Telemedizinführer Deutschland, Ausgabe 2007

Kontakt/Autor(en): Michael Herfert, Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Darmstadt

Seitenzahl:

5

Sonstiges:

3 Abb., 2 Tabellen

Dateityp/ -größe:

PDF / 333 kB

Click&Buy-Preis in Euro:

0,50

Ä Rechtlicher Hinweis:

Ein Herunterladen des Dokuments ist ausschließlich zum persönlichen Gebrauch erlaubt. Jede Art der Weiterverbreitung oder Weiterverarbeitung ist untersagt. Ä

Hier gehts zum Click&Buy-Download... Ä Allgemeine Infos zu Click&Buy finden Sie hier... Ä