Norbert Pohlmann

Beweissicherheit der EDV am Beispiel veränderter Dokumentation (II)

In der ersten Folge dieses Beitrags (vgl. IT-Sicherheit & Datenschutz 9/2007) hatten wir die wesentlichen Gründe für den Übergang zur elektronischen Datenhaltung im Gesundheitswesen erörtert und die wesentlichen Anforderungen an ein solches Archiv beschrieben. Im abschließenden zweiten Teil wollen wir zeigen, wie sich diese umsetzen lassen.

Im Detail niedergelegt sind diese Anforderungen und Regeln zu ihrer Umsetzung den bereits erwähnten Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS). Deren Kern hat der Verband Organisations- und Informationssysteme e.V. (VOI) in folgenden zehn Merksätzen zusammengefasst:

- Jedes Dokument muss unveränderbar archiviert werden.
- Kein Dokument darf auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.
- Jedes Dokument muss mit geeigneten Retrievaltechniken (Suchfunktionen der Applikation oder des Archivierungsprogramms) wieder auffindbar sein.
- Es muss genau das Dokument wieder gefunden werden, das gesucht wurde.
- Die Zerstörung eines Dokuments während seiner vorgesehenen Lebensdauer muss ausgeschlossen sein.
- Jedes Dokument muss in genau der gleichen Form wieder angezeigt und gedruckt werden können, in der es erfasst wurde.
- Jedes Dokument muss zeitnah wiederauffindbar sein.
- Alle Aktionen im Archiv, die Veränderungen in der Organisation und Struktur bewirken, sind derart zu protokollieren, dass die Wiederherstellung des ursprünglichen Zustandes jederzeit möglich ist.
- Elektronische Archive sind so anzulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist.
- Das System muss dem Anwender die Möglichkeit bieten, die gesetzlichen Bestimmungen (BDSG, HGB/AO etc.) sowie die betrieblichen Bestimmungen des Anwenders hinsichtlich Datensicherheit und Datenschutz über die Lebensdauer des Archivs (Frage Böcker: Über dessen Lebensdauer hinweg oder über diese hinaus? Bitte klarstellen!) sicherzustellen.

Die Beweissicherheit des für die Dokumentation eingesetzten Verfahrens steht und fällt mit der Revisionssicherheit des Archivs. Das gilt auch im Gesundheitswesen, denn kann ein Systemadministrator oder eine andere Person Daten im Archiv ersetzen, so kann er dies auch im Auftrag oder aus Gefälligkeit für einen Arzt tun. Solche Manipulationen durch Dritte lassen sich jedoch in komplett „digitalisierten“ Archiven dank der eingesetzten elektronischen Signatur zuverlässig erkennen. Ärzte und Kliniken sollten ferner darauf achten, hierbei nur solche Techniken einzusetzen, die den speziellen Ansprüchen an die Langzeitarchivierung (für medizinische Dokumente wie etwa Krankenakten gelten derzeit i. d. R. Aufbewahrungsfristen von 30 Jahren) gerecht werden.

Archiv mit Zeitstempelfunktionen für signierte Dokumente

Verbessern lässt sich die Beweissicherheit zudem durch die Einbeziehung eines eindeutigen Zeitstempels: Will ein Benutzer ein Dokument in das Archiv einfügen, fordert die Anwendung einen Nachweis von einem Zeitstempel-Server an. Dieser Zeitstempel selbst verfügt ebenfalls über eine Signatur und ist damit seinerseits gegen absichtliche Veränderungen gesichert. Allerdings handelt es sich dabei nicht um eine qualifizierte elektronische Signatur, da diese laut Gesetz nur natürlichen Personen zusteht. Somit lässt sich die höchste denkbare Sicherheitsstufe nicht erreichen. Dieser „Mangel“ ist allerdings rein theoretischer Natur, in der Praxis gilt das beschriebene Verfahren als hinreichend manipulationsresistent. Das zeigt sich u. a. daran, dass es beispielsweise die Lottogesellschaften der Bundesländer nutzen, um den Eingang der Wettscheine – genauer: den Übermittlungszeitpunkt der angekreuzten Glückszahlen – festzuhalten.

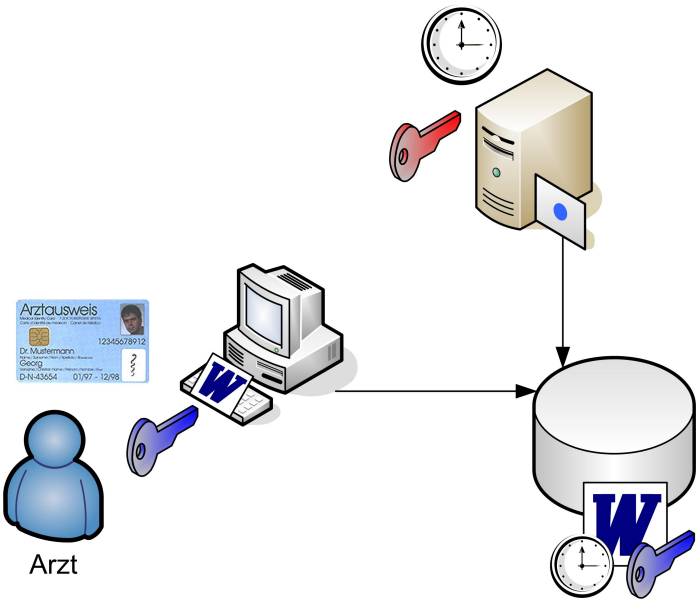

ABB. 1: Elektronische Archivierung mit Zeitstempel-Server

Einsatz von Massensignaturen

Noch komplizierter wird die Situation, wenn zudem traditionelle Papierdokumente in das elektronische Archiv überführt werden müssen. Wie bei Ämtern und Unternehmen nutzt man dafür auch im Gesundheitswesen massenweise Scans der vorhandenen Unterlagen. Um als beweissicher zu gelten, sind die dabei anfallenden OCR- und Bilddateien mit einer qualifizierten elektronischen Signatur zu versehen. Dafür wird gewöhnlich die Signatur des Mitarbeiters benutzt, der den Scanner bedient. Dieser so genannte Operator kontrolliert die gescannten Dokumente zudem stichprobenartig auf ihre Vollständigkeit und Unversehrtheit. Nach dem Signieren werden die Dokumente wieder an den Auftraggeber übermittelt. Dieser wiederum versieht sie mit einem eindeutigen Zeitstempel versehen und legt sie in seinem Archiv ab. Rechtsgrundlage dieser Verfahren ist nach Angaben der Hersteller einschlägiger Software-Lösungen, zu denen etwa die Düsseldorfer AuthentiDate International AG zählt, die Sozialversicherungs-Rechnungsverordnung (SVRV) nebst der zugehörigen Allgemeinen Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung (SRVwV), insbesondere deren § 36.

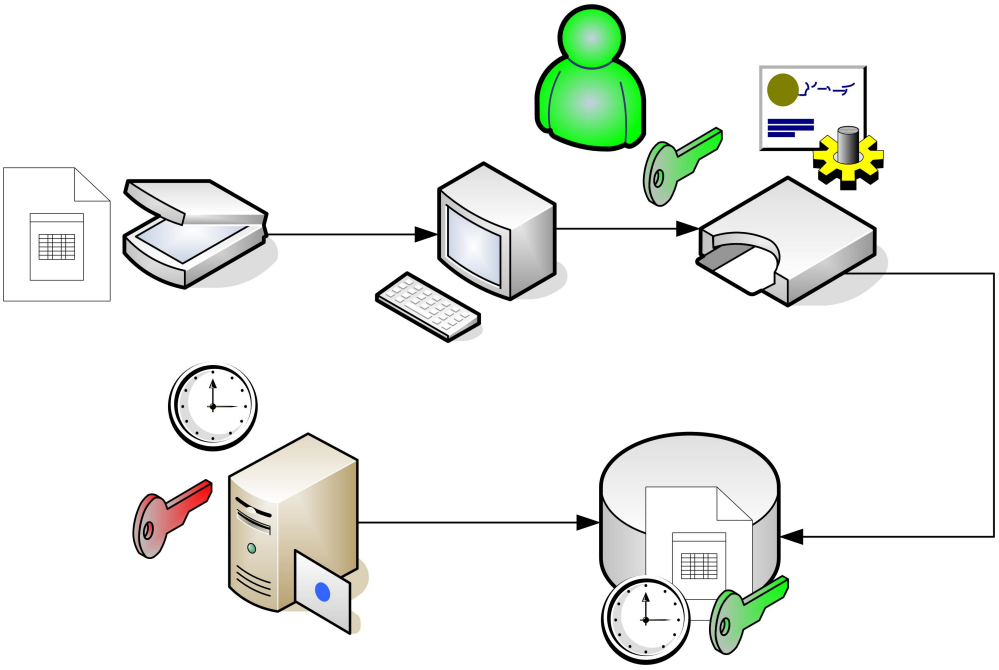

ABB. 5: Erstellung einer Massensignatur für gescannte Papierdokumente

Fazit

Zusammenfassend lässt sich feststellen, dass eine beweissichere Dokumentation bereits mit heute existierenden Archivierungslösungen realisierbar ist, sofern diese mit entsprechenden Funktionen für die Zugriffskontrolle und das Signieren von Dokumenten ausgestattet sind. Eine zentrale Rolle spielt dabei die qualifizierte elektronische Signatur, welche die Authentizität, Integrität und Verbindlichkeit der Dokumente sicherstellt. Besondere Anforderungen an das elektronische Archiv ergeben sich daraus, dass auch die zeitliche Einordnung der archivierten Dokumente möglich und eine spätere Manipulation ausgeschlossen sein muss. Das jeweils benutzte Verfahren sollte in einer eigenen Dokumentation genau erfasst und beschrieben werden. Sind diese Merkmale gegeben, kann eine elektronische Archivierungslösung mit hoher Wahrscheinlichkeit als hinreichend beweissicher gelten; im Zweifelsfall sollte ein Gutachter urteilen.

Im Gegensatz dazu ist bei der massenweisen Überführung von Papierdokumenten in elektronische Archive keine vergleichbare Sicherheit gegeben: Zwar haben sich die dabei gebräuchlichen Verfahren in der Praxis bewährt und basieren auf einschlägigen Verwaltungsvorschriften für das Gesundheitswesen. Damit existiert eine juristische Grundlage, auf die sich die „Archivbetreiber“ (also Ärzte und Kliniken) bei Auseinandersetzungen um die Beweiskraft eines medizinischen Dokuments stützen können. Aus technischer Sicht ist dies aber nur von begrenztem Wert. Denn das Hinzufügen einer qualifizierten elektronischen Signatur zu einem eingescannten Dokument stellt nur sicher, dass nachträgliche Änderungen auffallen. Ob bereits zuvor Röntgenbilder oder andere Bestandteile aus einer Krankenakte entfernt wurden, lässt sich so jedoch nicht feststellen. Ein weiterer Schwachpunkt besteht darin, dass bei derartigen Massenscans nur stichprobenartige Kontrollen der Dokumente auf Vollständigkeit und Unversehrtheit erfolgen.

((Info-Kasten:))

Elektronische Signatur

Zur Übermittlung von Geschäfts- und Verwaltungsdokumenten nutzen Behörden und Unternehmen heute bereits in vielen Fällen das Medium E-Mail. Neben der elektronischen Post in ihrer reinen Form schließt dies auch handschriftlich unterzeichnete Briefe sowie Faxe ein, die ggf. als Attachment übermittelt werden. Das ist juristisch nicht zu beanstanden, zumal ein rechtswirksames Handeln nach Ansicht von Experten wie dem auf das Recht der Informationstechnologie und die elektronische Kommunikation spezialisierten Hamburger Anwalt Ivo Geis „grundsätzlich formfrei“ ist. Eine

gewöhnliche E-Mail stellt demnach eine rechtswirksame Willenserklärung dar, mit der Rechte und Pflichten begründet werden.

Problematisch ist diese Auffassung deshalb, weil jede Mail während der Übermittlung abgefangen und verändert werden kann und die Absenderadresse kein hinreichender Nachweis ist, dass die Sendung auch tatsächlich von der dort genannten Person stammt. Im Klartext: Alle Bestandteile einer Mail – die Nachricht selbst, ihr Header und die beigefügten Anlagen – können gefälscht sein und werden von Kriminellen gefälscht. Um dieses Risiko zu minimieren bzw. auszuschließen, verwenden immer mehr Organisationen elektronische Signaturen. Diese ermöglichen dem Empfänger, die Integrität und Authentizität einer Mail zu überprüfen. Zusätzlich lassen sich Nachrichten mit ihrer Hilfe verschlüsseln.

Technik in Kürze

Elektronische Signaturen arbeiten mit Schlüsselpaaren. Dabei verfügt jeder Benutzer über einen öffentlichen und einen privaten Schlüssel. Für die Signatur wird von dem zu signierenden Dokument ein Hash-Wert gebildet, welcher dann mit dem privaten Schlüssel des Benutzers verschlüsselt wird. Diese Signatur wird zusammen mit dem Dokument verschickt. Der Empfänger erstellt ebenfalls einen Hash-Wert der Nachricht. Dann entschlüsselt er mit dem öffentlichen Schlüssel die Signatur des Benutzers und vergleicht beide Hash-Werte. Sind diese identisch, ist sowohl die Integrität des Dokuments als auch dessen Authentizität sichergestellt.

Signaturklassen

In Deutschland gibt es nach dem Signaturgesetz drei Klassen von Signaturen:

- **1. Klasse – Elektronische Signatur:** Hierbei handelt es sich um alle Daten, die einem Dokument beigefügt werden und zur Authentifizierung dienen, z.B. eine eingescannte Unterschrift oder eine Namenswiedergabe. Ob diese tatsächlich von der angegebenen Person stammen, ist jedoch nicht zweifelsfrei nachzuweisen; die Beweisqualität ist also als gering zu bewerten.

- **2. Klasse – Fortgeschrittene elektronische Signatur:** Diese muss ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sein und dessen Identifizierung ermöglichen. Der Schlüssel selbst sollte unter ständiger Kontrolle des Inhabers stehen. Die Signatur muss so mit den „Nutzdaten“ verknüpft sein, dass deren nachträgliche Veränderung erkennbar ist. Sie muss ferner von einem vertrauenswürdigen Dritten stammen, der als Zertifizierungsdienst fungiert und die Identität des Schlüsselinhabers (Absenders) verifiziert.

- **3. Klasse – Qualifizierte elektronische Signatur:** Die qualifizierte elektronische Signatur ist eine Weiterentwicklung der fortgeschrittenen elektronischen Signatur. Dabei gelten höhere Anforderungen an den Zertifizierungsdienst gestellt, der die Signatur ausgibt, insbesondere muss dieser von der Bundesnetzagentur akkreditiert sein. Jeder akkreditierte Zertifizierungsdienst erhält ein Gütezeichen nach §15 Abs. 1 Satz 4 SigG. Dieses besagt, dass die von diesen Anbietern ausgegebenen Zertifikate und die auf ihrer Basis erzeugten Signaturen eine „umfassende technische und administrative Sicherheit“ bieten. Da sich auch Anwender darauf berufen können, wird die Beweisführung vor Gericht erleichtert. Privatanwender können sich ihre Zertifikate in Deutschland u. a. bei ihrer Sparkasse, der Deutschen Bank, der Post und T-Systems beschaffen. Rechtsanwälte und Steuerberater erhalten sie außerdem bei der Datev.