Ursula Viebeg

Langzeitsicherung elektronisch signierter Dokumente

Die Umstellung auf elektronische Geschäftsprozesse ist inzwischen weit vorangeschritten. Die meisten geschäftsrelevanten Dokumente, wie Rechnungen, werden mittlerweile elektronisch erzeugt, empfangen und abgelegt, unabhängig von Branche und Unternehmensgröße. Der Gesetzgeber hat hierfür den rechtlichen Rahmen geschaffen: Das Signaturgesetz als Basis ermöglicht in vielen Bereichen eine rechtliche Gleichstellung von handschriftlichen Unterschriften und elektronischen Signaturen. Das neue Umsatzsteuergesetz beispielsweise fordert für die elektronische Rechnungsstellung qualifizierte elektronische Signaturen nach Signaturgesetz. Mit der Verabschiedung des Justizkommunikationsgesetzes wird die elektronische Kommunikation in der Justiz ermöglicht und geregelt. Im Verwaltungsbereich fördert die Initiative BundOnline 2005 elektronische Verwaltungsvorgänge und -dienstleistungen. Mit der Einführung der elektronischen Gesundheitskarte und dem elektronischen Heilberufsausweis erhalten über 200.000 Ärzte, 77.000 Zahnärzte und 20.000 Apotheker in den nächsten Jahren signaturfähige Smartcards. Die elektronische Signatur gewinnt somit auch in diesem Bereich zunehmend an Bedeutung. Erste signatur-relevante Anwendungen sind das elektronische Rezept und die elektronische Patientenakte.

In den genannten Anwendungsfeldern gelten rechtliche Aufbewahrungspflichten auch für elektronische Dokumente von teilweise über 30 Jahren. Hierbei sind folgende Anforderungen[1] zu erfüllen:

Die langfristig aufbewahrten elektronischen Dokumente sollen auch in mehreren Jahrzehnten noch lesbar und verarbeitbar sein und der rechtliche Beweiswert der Dokumente soll auf Dauer gesichert bleiben.

Bei Papierdokumenten sind diese Anforderungen leicht zu erfüllen. Handschriftlich unterschriebene Verträge sind auch nach Jahrzehnten noch gut lesbar und besitzen vor Gericht dieselbe Beweiskraft wie am Tag ihrer Ausstellung. Anders bei elektronisch signierten Dokumenten, die ihren Beweiswert verlieren, wenn sich das Dokumentenformat ändert oder die Signatur gefälscht werden kann.

Der Verlust der Fälschungssicherheit ist i. d. R. auf einen Alterungsprozess zurückzuführen, der sich wie folgt erklärt: Elektronische Signaturen basieren auf kryptografischen Algorithmen. Ein solcher Algorithmus gilt solange als sicher, wie die mit ihm erstellte Signatur nicht gefälscht werden kann. Eine Signatur ist fälschungssicher, wenn sie eindeutig einer Person zugeordnet und nur mit genau einem Dokument erfolgreich geprüft werden kann. Einem Angreifer darf es nicht möglich sein, eine falsche Identität anzunehmen oder weitere Dokumente zu finden, die ebenfalls zu der elektronischen Signatur „passen".

Rasant steigende Rechenkapazitäten und Fortschritte bei der Lösung mathematischer Verfahren zum Brechen der kryptografischen Algorithmen führen dazu, dass die verwendeten Signaturalgorithmen im Laufe der Zeit unsicher werden. Dieser Alterungsprozess wird bereits nach sechs Jahren signifikant und kann dazu führen, dass elektronisch signierte Dokumente ihre Beweiskraft einbüßen. Versäumt man, Maßnahmen für den Werterhalt elektronischer Signaturen zu treffen, kann ein elektronisch signiertes Dokument unter Umständen vor Gericht nicht mehr ausreichen, wenn man es nach einigen Jahren als Beweis vorlegen muss.

Eine weitere Herausforderung bei der Archivierung von elektronischen Dokumenten ist der Erhalt der Lesbarkeit der elektronischen Dokumentenformate. Niemand kann garantieren, dass nach einem Zeitraum von 30 Jahren noch Softwarekomponenten existieren, welche die damals verwendeten Datenformate verarbeiten und anzeigen können. Dies ist aber eine der Anforderungen an eine sichere Aufbewahrung von Dokumenten. Es ist daher zum einen erforderlich, Dokumente direkt in längerfristig gültigen Formaten zu erstellen. Zum anderen wird es notwendig sein, dauerhaft gespeicherte Dokumente im Laufe ihrer Aufbewahrungszeit rechtzeitig in andere, aktuellere Formate umzuwandeln. Auch die bereits existierende Vielzahl unterschiedlicher Dokumentenformate führt zu der Notwendigkeit, Dokumente in andere Formate umzuwandeln. Ein Beispiel sind Geschäftsprozesse mit unterschiedlichen Beteiligten, von denen nicht jeder jedes Format unterstützt. Bei signierten Dokumenten führt eine Formatumwandlung zu Problemen, denn sobald sich das Format eines Dokuments ändert, wird die ursprüngliche Signatur wertlos. Ohne

[1] Vgl. hierzu den Artikel in dieser Ausgabe zu: „Anforderungen und Trends der langfristigen Aufbewahrung von elektronischen Dokumenten" von Stefanie Fischer-Dieskau/Silke Jand/Michael Knopp/Alexander Roßnagel.

besondere Sicherheitsvorkehrungen ist die rechtliche Aussagekraft des umgewandelten (transformierten) Dokuments fraglich.

Das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) arbeitet seit Jahren an der Lösung der genannten Probleme. SIT beteiligt sich an Forschungsprojekten, fungiert als Berater auf diesem Gebiet und entwickelt einsetzbare Lösungen.

Konzept: Langzeitsicherung elektronisch signierter Dokumente durch Signaturerneuerung

Im Forschungsprojekt ArchiSig (2001-2003) hat SIT zusammen mit Partnern eine Lösung zum dauerhaften Erhalt des Beweiswerts elektronischer Signaturen entwickelt. Das Verfahren beruht auf der rechtzeitigen Erneuerung von Signaturen. Rechtzeitig bedeutet bevor die verwendeten Signaturalgorithmen unsicher werden. Wie lange die einzelnen Signaturalgorithmen als sicher anzusehen sind, wird jährlich von der Bundesnetzagentur festgestellt. Sie veröffentlicht eine Liste der geeigneten Signaturalgorithmen, wobei die Dauer der Sicherheitseignung der Algorithmen für einen Zeitraum von jeweils sechs Jahren prognostiziert wird.

Das in ArchiSig entwickelte Verfahren ist automatisierbar, da die Erneuerung nicht durch den ursprünglichen Signierer erfolgen muss, sondern von einer Maschine geleistet werden kann. Nahe liegend ist die Benutzung eines Zeitstempeldienstes, welcher den Hashwert eines Dokuments, d.h. ein Komprimat des Dokuments, erhält, die aktuelle Zeit hinzufügt und das so entstandene Konstrukt mit seiner eigenen, auf aktuellen Algorithmen und Schlüssellängen beruhenden, elektronischen Signatur versieht. Aus Kosten- und Optimierungsgründen wird ein Zeitstempel für möglichst viele Dokumente eingeholt. Hierzu werden die einzelnen Dokumente mit einem so genannten Hashverfahren komprimiert und die entstehenden Hashwerte in einer Baumstruktur zusammengefasst (siehe Abb. 1).

Nur für den obersten Hashwert des Baumes wird dann ein Zeitstempel eingeholt, dieser erneuert die Signaturen aller Dokumente des Baumes. Ein Zeitstempel enthält wiederum eine Signatur, unterliegt also seinerseits einem Alterungsprozess und muss regelmäßig erneuert werden. Auf diese Weise entsteht im Laufe der Zeit eine Kette von Zeitstempeln, die zusammen den Beweiswert der Dokumente sichern. Das Verfahren ist massentauglich, effizient, kostengünstig und erfüllt die Anforderungen des Signaturgesetzes.[2] Entscheidend ist, dass die Signaturerneuerung stets rechtzeitig vorgenommen wird, bevor die eingesetzten Algorithmen ihre Beweiskraft verlieren und die Signaturen gefälscht werden können. Nur dadurch lässt sich eine kryptographiebasierte Argumentationslinie aufrechterhalten. Die Beweiswerterhaltung elektronischer Signaturen ist damit nicht an einen einmaligen Vorgang geknüpft, sondern an einen kontinuierlichen Prozess, der integraler Bestandteil eines Archivierungskonzeptes sein sollte.

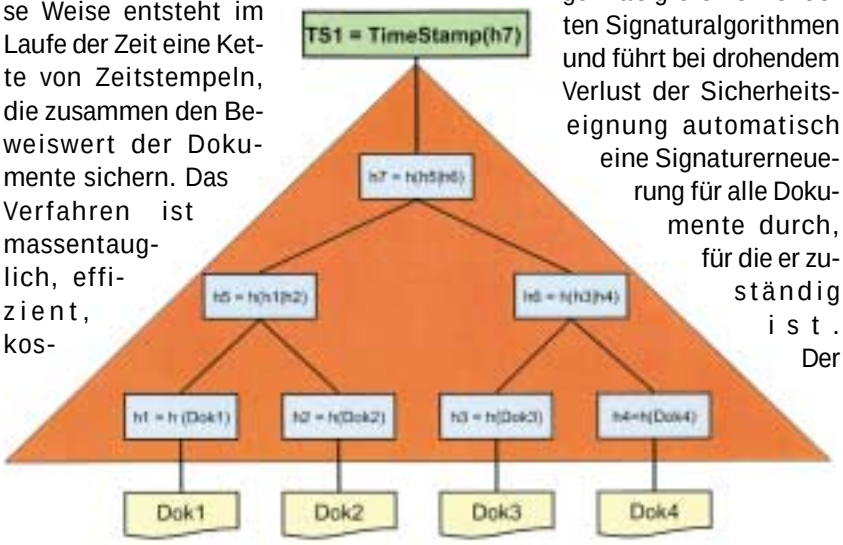

Abb. 1: Ein Hashbaum fasst sehr viele Dokumente zusammen. Die Wurzel (hier h7) repräsentiert alle Dokumente. Nur für sie wird ein Zeitstempel (TS1) eingeholt.

Softwareprodukt *ArchiSoft*

Das Fraunhofer-Institut SIT bietet mit seinem Softwaresystem *ArchiSoft*[3] ein Produkt an, das die Lösungskonzepte des Forschungsprojekts ArchiSig umsetzt. Die wesentlichen Komponenten sind ein Server zur Langzeit-Beweiswerterhaltung und ein Client zur späteren Verifikation der archivierten und signierten Dokumente. Der Server überprüft regelmäßig die verwendeten Signaturalgorithmen und führt bei drohendem Verlust der Sicherheitseignung automatisch eine Signaturerneuerung für alle Dokumente durch, für die er zuständig ist. Der ArchiSoft-Server ist vollständig prozessgesteuert und lässt sich leicht in bestehende Archivierungs- und Dokumentenmanagementsysteme (DMS) integrieren. Die entstehenden Zeitstempelketten werden in einem standardisierten Format[4] abgelegt, so dass die Verifikation auch mit anderen Standard-konformen Produkten

[2] Siehe hierzu das Gutachten von Prof. Alexander Rossnagel unter: http://www.teletrust.de/fileadmin/files/ag8_isis-mtt-gutachten-langzeitsig.pdf.

[3] Siehe hierzu: http://www.sit.fraunhofer.de/archisoft.

[4] http://www.ietf.org/internet-drafts/draft-ietf-ltans-ers-05.txt

erfolgen kann. ArchiSoft ist auch für die Verwaltung nicht signierter Dokumente einsetzbar. Ein Krankenhaus beispielsweise könnte mit seiner Hilfe auch in vielen Jahren nachweisen, zu welchem Zeitpunkt welche Untersuchungsergebnisse (signiert oder nicht signiert) vorgelegen haben.

Für das Problem der Alterung von elektronischen Signaturen existiert somit eine wirkungsvolle Lösung.

Transformation signierter Dokumente

Das Problem, das bei Formatumwandlungen (Transformationen) von signierten Dokumenten auftritt, ist noch offen. Das Brechen der Signatur tritt nicht nur bei Transformationen von einem elektronischen Format in ein anderes auf. Ein ähnliches Problem entsteht bei der Digitalisierung von Papierdokumenten. Wird beispielsweise eine von Hand unterschriebene Patientenakte digitalisiert, verliert die Unterschrift ebenfalls ihre Gültigkeit. Zudem besteht in bestimmen Anwendungskontexten die Notwendigkeit für Transformationen, wenn aus Gründen des Datenschutzes personenbezogene Daten geschwärzt werden. Medizinische Dokumente (z. B. Patientenakten) müssen, wenn sie in der wissenschaftlichen Forschung eingesetzt werden sollen, aus datenschutzrechtlichen Gründen anonymisiert und pseudonymisiert werden.

Regelungen und Verfahren werden daher benötigt, die eine rechtssichere Transformation signierter Dokumente ermöglicht.

Das vom Bundeswirtschaftsministerium geförderte Projekt TransiDoc (www.transidoc.de) „Rechtssichere Transformation signierter Dokumente“ unter der Federführung des Fraunhofer SIT greift dieses Problem auf. Neben technischen Lösungen für die Anwendungsbereiche Bauverwaltung, Gesundheitswesen und Notariate wird auch ein Katalog von Verfahrensvorschriften für eine rechtssichere Transformation signierter Dokumente entwickelt. Gleichzeitig werden die rechtlichen Rahmenbedingungen aufgezeigt, wobei sowohl die Handlungsmöglichkeiten im bestehenden Rechtsrahmen berücksichtigt werden, als auch Vorschläge für einen weiteren Gesetzgebungsbedarf entwickelt werden.

Unter einer Transformation wird die Umwandlung eines Ausgangsdokuments in ein Zieldokument verstanden. In TransiDoc werden konzeptionell drei Transformationsarten betrachtet. Hierzu gehören Transformationen von elektronischen in elektronische Dokumente (E®E), und solche, an denen Papierdokumente beteiligt sind (E®P, P®E). Eine Transformation hat immer einen bestimmten Zweck, der sich daraus ergibt, wozu das Zieldokument dienen soll. Bei der Digitalisierung von Papierbeständen beispielsweise ist der Zweck der Transformation, einen digitalen Ersatz für die Papierdokumente zu erhalten. Ziel einer sicheren Transformation signierter Dokumente ist, das Zieldokument seinem Zweck entsprechend verwenden zu können, auch wenn das Ausgangsdokument nicht vorliegt. Voraussetzung hierfür ist, dass dem Zieldokument ein vergleichbarer Beweiswert zukommt wie dem Ausgangsdokument. Es müssen daher adäquate Mittel gefunden werden, die dem transformierten Dokument die gleiche rechtliche Sicherheit geben, wie die ursprüngliche Signatur dem Ausgangsdokument.

Kernpunkt des Lösungsansatzes in TransiDoc ist es, spätere Gutachter in die Lage zu versetzen, nachzuvollziehen, was während einer Transformation mit dem Dokument geschah. Bei einer nachträglichen Prüfung des Zieldokuments sollen unter anderen folgende Fragen beantwortet werden können:

- Welche Transformation wurde vorgenommen?
- Wer hat das Ausgangsdokument unterschrieben bzw. signiert?
- Wer hat die Transformation durchgeführt?
- War die betreffende Person dazu autorisiert?

Das Zieldokument muss daher neben den transformierten Inhalten auch Ablaufprotokolle und Prüfungsergebnisse, wie z. B. Ergebnis der Signaturverifikation, und zur Sicherung der Daten auch elektronische Signaturen enthalten. Leitkonzept von TransiDoc ist das „Transformationssiegel“ – ein mit einer elektronischen Signatur versehener Vermerk, der die oben gestellten Fragen beantwortet und Bestandteil des Zieldokuments ist. Das Transformationssiegel sichert die transformierten Inhalte, ermöglicht die nachträgliche Überprüfbarkeit, bestätigt die Korrektheit der Transformation und garantiert die Vertrauenswürdigkeit durch eine nichtabstreitbare Zuordnung der Transformation zur transformierenden Entität oder Person. Diese Möglichkeit der A-posteriori-Überprüfung ist der wichtigste Baustein für die Beweiskraft des Zieldokuments. Damit könnte ein transformiertes Dokument rechtlich gesehen ebenso genutzt werden wie sein Original.

Ursula Viebeg ist wissenschaftlich-technische Mitarbeiterin am "Fraunhofer-Institut für Sichere Informationstechnologie SIT". Ihre Arbeits- und Forschungschwerpunkte der letzten Jahre sind: elektronische Signaturen, Public-Key-Infrastrukturen und Langzeitarchivierung elektronisch signierter Dokumente. Sie ist Mitglied des AWV-Arbeitskreises 6.3 „Daten- und Speichermanagement“.