c't 23/2003, S. 40: Digitale Signatur



**Christiane Schulzki-Haddouti**

# Bedingt gerichtsfest

## Studie testet Beweiskraft digitaler Signaturen

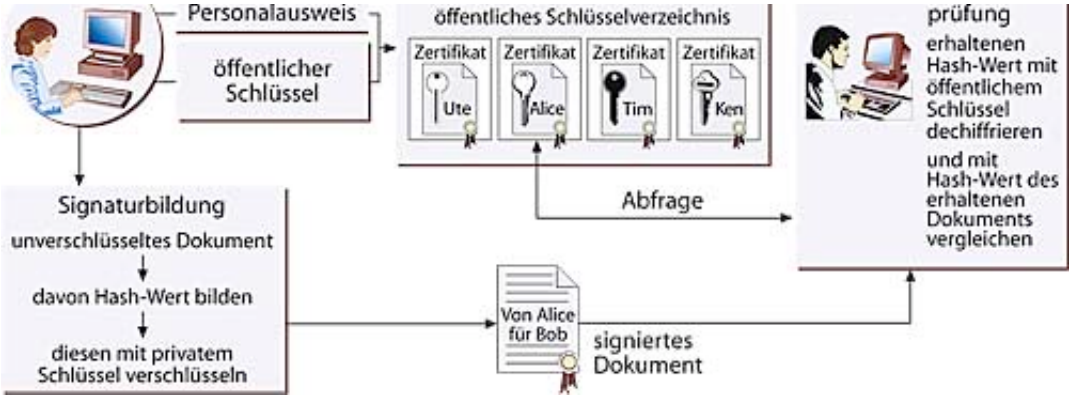
**Wenn digitale Signaturen die Unterschrift von Hand wirklich überall ersetzen sollen, müssen sie auch den Ansprüchen an ein Beweismittel genügen. In simulierten Gerichtsverfahren prüften Richter unterschiedlich archivierte elektronisch signierte Dokumente.**

Digitale Signaturen sind nicht für die Ewigkeit gebaut. Gerade einmal fünf Jahre lang sind qualifizierte Signaturen bei nicht akkreditierten Zertifizierungsdiensteanbietern verfügbar und prüfbar, bei akkreditierten sind es immerhin 30 Jahre. Dokumente über die Rechtsstellung eines Menschen müssen allerdings unter Umständen ein ganzes Menschenleben aufbewahrt werden - geht es um Rechte an einem Grundstück oder Gebäude, unter Umständen sogar weit mehr als ein Jahrhundert. Auch Ärzte und Krankenhäuser haben ebenso wie Rechtsanwälte eine Dokumentationspflicht. Im Streitfall haben sie deshalb die Beweislast.

Doch wie beweissicher sind digital signierte Dokumente? Und wie sorgt man dafür, dass sie es auch in Jahrzehnten noch sind? Die Projektgruppe verfassungsverträgliche Technikgestaltung (provet) unter der Leitung von Alexander Roßnagel, Juraprofessor an der Universität Kassel, und das Darmstädter Fraunhofer Institut Sichere Telekooperation (SIT) simulierten, wann digital signierte Unterlagen vor Gericht Bestand haben können: Richter, Rechtsanwälte und Gutachter überprüften Mitte Oktober in Heidelberg in zwölf gerichtlichen Testverfahren, deren Streitgegenstand realistischen Fällen nachgestellt war, ob sie die vorgelegten - künstlich gealterten - elektronisch signierten Dokumente als Beweismittel anerkennen könnten.

Wie man handschriftlich signierte Papierurkunden aufbewahrt, weiß man seit Jahrhunderten. „Für die langfristige Aufbewahrung elektronisch signierter Dokumente gibt es bisher nur die Erkenntnis, dass dies ein noch ungelöstes Problem ist“, sagt Alexander Roßnagel.

Generell geht es bei der Langzeitarchivierung um drei Probleme: Zum einen muss der Dokumentenbesitzer einen Überblick über die Sicherheitseignung der digitalen Signatur behalten. Mit dem Fortschritt der Rechnertechnologie verlieren die der Signatur zugrunde liegenden kryptographischen Verfahren an Sicherheit. Die Signaturen müssen deshalb immer wieder mit besseren Algorithmen neu „versiegelt“ werden.




**Die für die elektronische Signatur verwendeten Verschlüsselungsverfahren und Zertifikate gelten nicht für die Ewigkeit.**

Zum anderen läuft auch die Frist irgendwann ab, innerhalb der die Zertifikate geprüft werden können, die die Zugehörigkeit einer Signatur zu einer Person bestätigen. Deshalb muss der Besitzer für die Prüfung der Authentizität des Dokuments rechtzeitig vor Ablauf dieser Fristen bei den jeweiligen Zertifizierungsstellen die Verifikationsdaten einholen, um die Gültigkeit der Zertifikatsdaten aus Wurzel-, Aussteller- und Nutzerzertifikat zu prüfen. Wenn abzusehen ist, dass deren Gültigkeitsdauer demnächst abläuft, muss der Inhaber der Dokumente diese ebenfalls neu signieren.

Schließlich muss er noch nachweisen, dass das Dokument nie durch ein ungeeignetes Kryptoverfahren geschützt wurde, also garantiert unverändert erhalten geblieben ist. Für Einzelpersonen mit wenigen Dokumenten ist ein solcher Aufwand noch von Hand zu bewältigen. Professionelle Einrichtungen dürften dagegen ohne ein automatisiertes Verfahren kaum zurechtkommen.

Das vom Bundeswirtschaftsministerium geförderte Konsortialprojekt „Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente (ArchiSig)“ hat nun ein Konzept für die rechtssichere Langzeitaufbewahrung elektronisch signierter Dokumente entwickelt. Es ist auch für große elektronische Archive geeignet. Ein Prototyp wird derzeit im Universitätsklinikum Heidelberg erprobt. Das ArchiSig-System erhebt automatisch die notwendigen Verifikationsdaten, aktualisiert sie regelmäßig und speichert sie zusammen mit dem Dokument. Es erkennt die auslaufende Sicherheitseignung von Signaturen und signiert rechtzeitig alle betroffenen Dokumente erneut.

## Testprozess

Für die in den simulierten Gerichtsverhandlungen geprüften Dokumente führten Provet und das Fraunhofer Institut verschiedene Archivierungsverfahren für einen Zeitraum von über 40 Jahren im „Zeitraffer“ durch. Sie legten den Richtern Beweisstücke vor, die mit ArchiSig archiviert wurden, aber auch welche, bei denen Neusignierungen oder Verifikationsdaten fehlten.

In einem der Beispielprozesse klagte ein Herr Teron gegen die Berufsgenossenschaft wegen seiner Berufsunfähigkeitsrente. Er führte eine unheilbare Lungenschädigung darauf zurück, dass er vor 30 Jahren asbesthaltige Materialien verarbeiten musste. Zu dem Prozess kam es, weil die Berufsgenossenschaft sich auf elektronische Ergebnisberichte der damaligen Routineuntersuchungen aus ihrem Archiv stützte, nach denen keine

Auffälligkeiten festgestellt wurden. Herr Teron legte dagegen für seinen Anspruch den elektronischen Bericht einer privatärztlichen Untersuchung vor, die damals schon einschlägige Anfangsschädigungen feststellte.

Die Berufsgenossenschaft zweifelte an der Echtheit dieses Berichts und schloss sogar eine Fälschung durch Herrn Teron nicht aus. In der Simulation hat Herr Teron den Prozess verloren. Während die Berufsgenossenschaft ihre Dokumente mit ArchiSig aufbewahrt hatte, konnte er nur vortragen, seine Dokumente 30 Jahre auf seinen Festplatten gespeichert zu haben. Dies war dem Richter trotz Signatur für einen Echtheitsbeweis zu wenig. In der Realität sähe Herr Teron nun wegen des Verdachts auf Dokumentenfälschung einem Strafprozess entgegen.

Dokumente, die fehlerhaft archiviert wurden, fassten die Richter generell erst einmal „mit spitzen Fingern“ an. „In solchen Fällen gab es keine Beweissicherheit“, sagte Roßnagel. Die Richter prüften dann, ob der Besitzer etwa ein Motiv für eine Dokumentenfälschung hatte und ob er überhaupt fähig war, ein digitales Dokument zu fälschen. Durchgängig signierte Dokumente hingegen erkannten die Richter immer an. Kein Problem hätte Herr Teron natürlich auch dann gehabt, hätte er den Original-Untersuchungsbericht auf Papier vorlegen können. (anm)

---

**Kommentare:**

Re: Sicherheit bei digitalen Daten? (101 5.12.2003 16:59)
Na, da haben sich ja zwei gefunden.... (Jago 12.11.2003 15:24)
Ja. Du! Wofür ich Dir auch zu Dank verpflichtet bin. (Go4HESY 12.11.2003 10:01)
mehr...