Rolf Oppliger

Digitale Dokumente – Alte und neue Herausforderungen sowie Lösungsansätze

Referat an der Tagung für Informatik und Recht, Bern, 26. Oktober 2004

Digitale Dokumente spielen im wirtschaftlichen und gesellschaftlichen Leben eine zunehmend wichtige Rolle. In diesem Beitrag werden die alten und neuen Herausforderungen sowie Lösungsansätze für digitale Dokumente aufgezeigt und diskutiert. Dabei kommt der Beitrag zum Schluss, dass sich der sinnvolle und sichere Einsatz und Umgang mit digitalen Dokumenten in den nächsten Jahrzehnten noch herausbilden muss, und dass wir diesbezüglich wohl erst am Anfang einer langen Entwicklung stehen.

Digital information lasts forever – or five years, whichever comes first.

– Jeff Rothenberg (2001)

Inhaltsübersicht

I. Einführung

[Rz 1] Der Begriff Dokument stammt ursprünglich aus dem Lateinischen und steht für Urkunde, Beweisstück oder Beweis. Heute wird der Begriff meist weiter gefasst und es werden darunter auch andere Formen von materiell dargestellter Information verstanden. Beispiele sind Papierdokumente aller Art, Fotos, Filmrollen und Tonträger. Charakteristisch an einem solchen Dokument im herkömmlichen Sinn ist in jedem Fall die Zusammenlegung und Nichtunterscheidbarkeit von Struktur, Inhalt und Layout.

[Rz 2] Als digitale Dokumente kann man alle Formen von nicht materiell (d.h. immateriell) bzw. digital dargestellter Information verstehen. Beispiele sind Text-, Bild-, Video- und Audiodateien. Grundsätzlich lässt sich jede Art von Information digital – d.h. als digitales Dokument – darstellen. Ein in Zukunft wichtiges Beispiel stellt Geld dar. Geld repräsentiert Information und diese Information lässt sich letztlich auch als digitales Dokument (in Form von digitalem Geld) darstellen. Im Gegensatz zu herkömmlichen Dokumenten wird bei einem digitalen Dokument meist zwischen Struktur, Inhalt und Layout unterschieden. Dabei gibt es viele (formale) Sprachen, die einzelne oder auch alle Aspekte abdecken und unterstützen. Eine besondere Bedeutung kommt in diesem Zusammenhang der eXtensible Markup Language (XML) zu[1]. XML hat sich in der jüngeren Vergangenheit insbesondere im Zusammenhang mit Web-basierten Diensten (sogenannten «Web Services») zu einem eigentlichen Schlagwort entwickelt.

[Rz 3] Jedes (herkömmliche oder digitale) Dokument hat einen Lebenszyklus. Demnach lassen sich etwa die folgenden vier Phasen unterscheiden:

- Erstellungsphase: In dieser Phase wird das Dokument erstellt.
- (Aktive) Nutzungsphase: In dieser Phase wird das Dokument aktiv genutzt.
- (Passive) Archivierungsphase: In dieser Phase wird das Dokument nicht mehr aktiv genutzt, sondern nur noch passiv aufbewahrt (d.h. archiviert).
- Zerstörungsphase: In dieser Phase wird das Dokument zerstört.

[Rz 4] Im Gegensatz zu herkömmlichen Dokumenten sind bei digitalen Dokumenten die verschiedenen Phasen teilweise nicht mehr klar voneinander abgrenzbar. So ist z.B. die Abgrenzung zwischen der aktiven Nutzungsphase und der passiven Archivierungsphase eines digitalen Dokumentes in zunehmendem Masse unklar. Ist eine Datei, die zwar auf einer Festplatte gespeichert ist, auf die aber während Monaten nicht mehr zugegriffen worden ist (ausser vielleicht für Backup-Zwecke) noch in der Nutzungsphase oder befindet sie sich bereits in der Archivierungsphase? Was ist, wenn das Dokument auf ein sekundäres Speichermedium (z.B. CD-ROM oder DVD) ausgelagert worden ist? Was ist, wenn beide Speicherformen koexistieren? Ähnliches gilt für den Zeitpunkt der Zerstörung eines digitalen Dokumentes. Von einem solchen Dokument gibt es möglicherweise sehr viele Kopien und die Zerstörung des Dokumentes würde eigentlich die Zerstörung aller Kopien mit einschliessen. Leider ist es in der Praxis oft schwierig und kaum möglich zu sagen, wo überall wie viele Kopien eines digitalen Dokumentes erstellt und angelegt worden sind. Zudem gibt es von den meisten in Bearbeitung befindlichen Dokumenten temporäre Kopien, die automatisch und für den Benutzer transparent vom Betriebssystem oder der Anwendungssoftware angelegt werden. Oft können im Rahmen von forensischen Untersuchungen an sich zerstörte Dateien über solche temporäre [2]Kopien wieder rekonstruiert werden.

II. Rechtliche Rahmenbedingungen

[Rz 5] In der Schweiz sind seit dem 1. Juni 2002 neue Bestimmungen des Obligationenrechts über die kaufmännische Buchführung bzw. die ordnungsgemässe Führung und Aufbewahrung der Bücher, Korrespondenz und Belege (Art. 957-963 OR) in Kraft. Ergänzt werden diese neuen Bestimmungen des Obligationenrechts durch eine Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (Geschäftsbücherverordnung, GeBüV).

[Rz 6] Mit den neuen Bestimmungen des Obligationenrechts und der GeBüV ist die rechtliche Grundlage geschaffen, damit Geschäftsbücher, Geschäftskorrespondenz und Belege nicht nur auf Papier, sondern auch als digitale Dokumente und auf anderen Informationsträgern geführt und aufbewahrt werden können. Zudem ist festgelegt, wann – d.h. unter welchen Voraussetzungen – veränderbare Informationsträger als Speichermedium zur Archivierung zugelassen sind (z.B. digitale Signatur, Zeitstempel, Audit-Log...). Die Voraussetzungen sind allerdings auf einem hohen Abstraktionsniveau verfasst, so dass eine Umsetzung in jedem Fall noch viele Konkretisierungen erforderlich macht.

[Rz 7] Im Bereich der digitalen Signatur werden voraussichtlich auf den 1. Januar 2005 das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES), die Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES), sowie die technischen und administrativen Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur des BAKOM in Kraft treten [3]. Damit werden auch in der Schweiz die rechtlichen Voraussetzungen gegeben sein, damit den handschriftlichen Unterschriften gleichgestellte elektronische Signaturen eingesetzt werden können. Ob und wenn ja wann sich im Sinne des ZertES/VZertES anerkannte elektronische Signaturen im praktischen Einsatz durchsetzen werden, ist zurzeit offen. Jedenfalls gibt es bis zum heutigen Zeitpunkt keinen Zertifizierungsdiensteanbieter, der entsprechende qualifizierte digitale Zertifikate ausgeben kann. Bis es in der Schweiz derartige Zertifizierungsdiensteanbieter gibt, werden für konkrete Fragestellungen Übergangslösungen gesucht und akzeptiert werden müssen. So akzeptiert z.B. die ESTV – gestützt auf die seit dem 1. März 2002 geltende Verordnung des EFD über elektronisch übermittelte Daten und Informationen (ElDI-V) – für Mehrwertsteuerabrechnungen Zertifikate der deutschen Firma TC TrustCenter AG.

III. Alte Herausforderungen und Lösungsansätze

[Rz 8] Es gibt sicherheitstechnische Herausforderungen an digitale Dokumente, die sich von den Herausforderungen

an herkömmliche Dokumente grundsätzlich nicht unterscheiden. In diesem Sinn «alte» Herausforderungen betreffen die Vertraulichkeit (Abschnitt 3.1), die Authentizität, Integrität und Verbindlichkeit (Abschnitt 3.2), die Autorisation und Zugriffskontrolle (Abschnitt 3.3), sowie die Verfügbarkeit (Abschnitt 3.4) von Dokumenten. Auf diese Punkte wird im Folgenden kurz eingegangen.

1. Vertraulichkeit

[Rz 9] Im Umgang mit herkömmlichen Dokumenten kennen wir uns mit Vertraulichkeitsanforderungen relativ gut aus. Wir klassifizieren Dokumente und gehen der Klassifikation entsprechend mit ihnen um. Wir setzen physische Schutzmassnahmen ein und kennen uns mit einschlägigen Massnahmen aus dem Bereich der Informationssicherheit relativ gut aus. Vieles geschieht intuitiv, ohne dass wir uns dessen bewusst sind. Wenn wir z.B. im täglichen Leben einen Brief für den Postversand in einen Umschlag stecken, dann geschieht dies eigentlich zum Zweck des Vertraulichkeitsschutzes (ohne dass wir uns dessen bewusst sind).

[Rz 10] Auch digitale Dokumente können sich durch bestimmte Vertraulichkeitsanforderungen auszeichnen. Allerdings ist ein Schutz hier nicht mit Hilfe von physischen Sicherheitsvorkehrungen und -massnahmen möglich. Stattdessen müssen logische Sicherheitsmassnahmen – in Form von Verschlüsselungsverfahren – eingesetzt werden, um digitale Dokumente wirksam vor Auslesen zu schützen. Solche Verfahren sind seit Jahrzehnten Gegenstand der kryptografischen Forschung und Entwicklung. Sie gelten heute als relativ gut verstanden.

2. Authentizität, Integrität und Verbindlichkeit

[Rz 11] Im Umgang mit herkömmlichen Dokumenten haben sich verschiedene Verfahren zur Sicherstellung der Authentizität, Integrität und Verbindlichkeit herausgebildet. Man denke hier etwa an handschriftliche Unterschriften, «offizielles» Briefpapier, Siegel oder andere optische Erkennungsmerkmale bzw. an physikalische Dokumenteigenschaften und -merkmale von Dokumenten, die man im Streitfall heranziehen kann (z.B. Alter von Papier und Tinte).

[Rz 12] Digitale Dokumente haben mindestens gleich hohe Anforderungen an die Authentizität, Integrität und Verbindlichkeit wie herkömmliche Dokumente. Dabei hat man das spezielle Problem, dass digitale Dokumente selbst keine physikalischen Eigenschaften haben, und dass man sich mit kryptografischen Verfahren entsprechend behelfen muss. Dabei können Nachrichtenauthentifikationscodes (MACs), digitale Signaturen, Zeitstempel, Sende- und Empfangsbestätigungen sowie Aufzeichnungen aller Art (als Audit-Logs) eingesetzt werden, um die Authentizität, Integrität und Verbindlichkeit dieser Dokumente zu schützen. Aus technischer Sicht sind diese Verfahren relativ gut verstanden und etabliert. Aus juristischer Sicht sind sie wohl noch mit grossen Unsicherheiten und Fragen behaftet.

3. Autorisation und Zugriffskontrolle

[Rz 13] Im Umgang mit herkömmlichen Dokumenten ist es oft erforderlich, dass man die Zugriffsberechtigungen einschränkt und kontrolliert. Dies geschieht dann meist aufgrund einer explizit oder implizit durchgeführten Klassifikation und einer entsprechenden Handhabung der Dokumente (z.B. über Verteilerlisten).

[Rz 14] Für den Umgang mit digitalen Dokumenten beginnen sich verschiedene Ansätze zur Autorisation und Zugriffskontrolle herauszubilden. In einschlägigen Kreisen spricht man von Digital Rights Management (DRM). Dabei werden unter diesem Begriff verschiedene technologische Ansätze subsummiert. Microsoft hat z.B. für seine Windows-Plattform ein Rights Management System (RMS) [4] entwickelt und ist derzeit sehr stark damit beschäftigt, dieses RMS in verschiedenen Applikationen auch zu integrieren (bzw. diese Applikationen RMS-fähig zu machen). Andere Firmen fokussieren sich im DRM-Umfeld mehr auf Hardware-gestützte Ansätze, wie z.B. «Trusted Computing» (vgl. Abschnitt 4.1).

4. Verfügbarkeit

[Rz 15] Eine in der Praxis wichtige und grundlegende Anforderung an (herkömmliche und digitale) Dokumente betrifft die Verfügbarkeit. Wenn ein Dokument nicht verfügbar ist, dann nützt es letztlich nichts und seine Existenz

ist dann irrelevant.

[Rz 16] Sowohl bei herkömmlichen als auch bei digitalen Dokumenten kann die Verfügbarkeit eines Dokumentes durch Redundanz (im Sinne von Kopien) erhöht bzw. sichergestellt werden. Man beachte aber, dass Anforderungen an die Verfügbarkeit zuweilen auch in einem Zielkonflikt mit Anforderungen an die Vertraulichkeit stehen können. Wenn z.B. sehr viele Kopien eines Dokumentes angelegt, verteilt und abgelegt werden, dann muss sichergestellt sein, dass jede einzelne Kopie adäquat geschützt ist. Hier können wiederum kryptografische Verfahren zum Einsatz kommen (z.B. in Form von «Secret Sharing Schemes»).

IV. Neue Herausforderungen und Lösungsansätze

[Rz 17] Neben diesen «alten» Herausforderungen, gibt es im Bereich der digitalen Dokumente durchaus auch «neue» Herausforderungen. Im Folgenden werden drei solche neue Herausforderungen im Zusammenhang mit digitalen Dokumenten angesprochen. Es handelt sich dabei um den Schutz des geistigen Eigentums (Abschnitt 4.1), die Beweiskraft von digitalen Dokumenten (Abschnitt 4.2), sowie die Archivierung bzw. Relevanz und Vertrauenswürdigkeit von digitalen Dokumenten (Abschnitt 4.3). Diese neuen Herausforderungen zeichnen sich unter anderem dadurch aus, dass es noch kaum brauchbare Lösungsansätze gibt bzw. dass wir zurzeit erst daran sind, die eigentlichen Probleme zu verstehen.

1. Schutz des geistigen Eigentums

[Rz 18] Im Gegensatz zu herkömmlichen Dokumenten können digitale Dokumente verlustfrei kopiert und weiterverbreitet werden, d.h. es gibt keine qualitativen Unterschiede zwischen einem Original und der (den) Kopie(n). Damit ist dem Missbrauch Tür und Tor geöffnet und es stellt sich natürlich die Frage, wie das geistige Eigentum an digitalen Dokumenten wirksam geschützt werden kann. An dieser Frage sind naturgemäss die Anbieter von digitalen Dokumenten – d.h. die «Content Provider» – interessiert.

[Rz 19] Grundsätzlich gibt es hier «harte» und «weiche» Lösungsansätze:

- Bei einem harten Ansatz wird die Nutzung eines digitalen Dokumentes kontrolliert bzw. zu kontrollieren versucht (im angelsächsischen Raum spricht man in diesem Zusammenhang von «Usage Control»).
- Bei einem weichen Ansatz werden lediglich die Besitzverhältnisse am digitalen Dokument gekennzeichnet und auf geeignete Art und Weise im Dokument markiert (im angelsächsischen Raum spricht man in diesem Zusammenhang von «Digital Watermarking» oder «Digital Fingerprinting»).

[Rz 20] Der erste Ansatz erfreut sich derzeit – wie unter 3.3 angedeutet – im Rahmen der Bestrebungen um «Trusted Computing» grosser Popularität. Dabei ist nicht klar, ob und wenn ja in welchem Umfang sich Trusted Computing auf dem Massenmarkt durchsetzen kann. Der zweite Ansatz setzt voraus, dass sich die gekennzeichneten und im Dokument markierten Besitzverhältnisse juristisch auch durchsetzen lassen. Anderenfalls läuft der Ansatz ins Leere. Natürlich schliessen sich die beiden Lösungsansätze nicht aus und in der Praxis werden sie idealerweise miteinander kombiniert.

2. Beweiskraft von digitalen Dokumenten

[Rz 21] Herkömmliche Objekte (und Dokumente) haben eine durch die Physik bedingte eindeutige Darstellung, und diese Darstellung lässt in der Regel nur wenige mögliche und plausible Interpretationen zu. Demgegenüber hat ein digitales Objekt (und Dokument) viele mögliche Darstellungsformen und viele mögliche Interpretationen. Die jeweilige Darstellungsform hängt unter anderem auch von der eingesetzten Hard- und Software ab und ist damit inhärent mehrdeutig. Dies gilt entsprechend auch für die vielen Interpretationsmöglichkeiten.

[Rz 22] Solange die Dokumentenräume programmdisjunkt sind, resultiert aus der inhärenten Mehrdeutigkeit von digitalen Dokumenten kein Problem[5]. Sobald aber digitale Dokumente auftauchen, die mit verschiedenen Programmen dargestellt unterschiedliche Informationen darstellen, wird man (auch juristische) Probleme haben. Man beachte, dass solche Programme durchaus auch künstlich erzeugt werden können. So ist z.B. der Fall denkbar,

in dem ein Angeklagter, dem vorgeworfen wird, ein bestimmtes Dokument digital signiert zu haben, ein Programm entwickelt, mit dem die gleiche Datei als Bild interpretiert eine (abstrakte) Grafik darstellt. Wer hat nun Recht? Wie kann man feststellen, was der Angeklagte zum Zeitpunkt der Signaturerstellung wirklich gemeint hat? Wie kann man das allenfalls beweisen? Vor diesem Hintergrund stellt sich natürlich die Frage, was man mit digitalen Dokumenten überhaupt beweisen kann bzw. wie man allenfalls die Beweiskraft von digitalen Dokumenten verbessern kann. Eine einfache Möglichkeit stellt z.B. die Einbindung von Meta-Information über das Dokument in die digitale Signatur dar. Eine aufwendigere Möglichkeit besteht darin, den Prozess der Signaturerstellung aufzuzeichnen.

3. Archivierung bzw. Relevanz und Vertrauenswürdigkeit

[Rz 23] Im Gegensatz zu herkömmlichen Dokumenten können digitale Dokumente einfach und kostenfrei in sehr grossen Mengen erzeugt werden, d.h. es gibt eine grosse Flut von digitalen Dokumenten. Damit stellt sich auf der einen Seite die Frage der Archivierung und auf der anderen Seite die Frage, wie man die Spreu vom Weizen trennt bzw. wie man überhaupt erkennen kann, ob ein digitales Dokument relevant und vertrauenswürdig ist.

- Aus praktischer Sicht ist die Frage der Archivierung relevant und akut. Archive haben heute im Prinzip zwei Möglichkeiten. Entweder archivieren sie mit den digitalen Dokumenten auch die entsprechenden Hard- und Softwarekomponenten, oder sie kopieren die archivierten digitalen Dokumente alle paar Jahre auf neue Datenformate und neue Datenträger um (das diesen Beitrag einleitende Zitat zielt auf diese Möglichkeit). Beide Möglichkeiten sind unzulänglich und die Langzeit-Archivierung von digitalen Dokumenten hat sich entsprechend zu einem wichtigen (und eigenständigen) Thema entwickelt.
- Auf dem Weg zur Informationsgesellschaft ist die Frage der Relevanz und Vertrauenswürdigkeit von digitalen Dokumenten eine zentrale. Vertrauenswürdigkeit hat mit Vertrauen zu tun und Vertrauen ist – im Gegensatz zur Sicherheit – nicht primär eine technische Fragestellung. Mit Ausnahme von ein paar Reputationssystemen sind in diesem Bereich noch kaum brauchbare Lösungsansätze bekannt.

[Rz 24] Dass sich die Relevanz und Vertrauenswürdigkeit von digitalen Dokumenten zu einer für die Informationsgesellschaft zentralen Frage entwickeln kann, hat sich vor kurzem gezeigt, als Unbekannte falsche Angaben über neue Ansätze für Ordnungsbussen im Strassenverkehr in Umlauf gesetzt haben [6]. Diese Falschmeldung hat in der Bevölkerung grosse Verunsicherung ausgelöst.

V. Schlussfolgerungen und Ausblick

[Rz 25] Digitale Dokumente bieten auf der einen Seite neue Chancen und Möglichkeiten, sind aber auf der anderen Seite auch mit neuen Gefahren und Risiken verbunden. Der sinnvolle und sichere Einsatz und Umgang mit digitalen Dokumenten wird sich in den nächsten Jahrzehnten noch herausbilden (müssen). Wir sind erst am Anfang einer langen Entwicklung und haben gerade erst begonnen, die Probleme zu erfassen (z.B. im Zusammenhang mit der Langzeit-Archivierung von digitalen Dokumenten). Viele der Probleme erscheinen zwar schwierig aber nicht unlösbar. Es ist möglich und sogar wahrscheinlich, dass künftige Generationen mit digitalen Dokumenten ähnlich selbstverständlich umgehen werden wie wir heute mit herkömmlichen Dokumenten. Der Weg dorthin wird aber lang sein und gepflastert mit Schwierigkeiten und zum Teil sehr speziellen Herausforderungen.

PD Dr. Rolf Oppliger ist Mitarbeiter des Informatikstrategieorgans Bund (ISB), führt eSECURITY Technologies Rolf Oppliger, ist Privatdozent an der Universität Zürich und gibt im U.S. amerikanischen Artech House Verlag eine Bücherreihe zum Thema Computersicherheit heraus.

Résumé français de l’exposé de Rolf Oppliger aux Journées d’informatique juridique 2004 à Berne: Anne Cherbuin, Documents électroniques: anciens et nouveaux défis, esquisses de solutions, in: Jusletter 8. November 2004.

1

Extensible Markup Language, zum Austausch und zur Speicherung von strukturierten, hierarchisch geordneten Daten (http://www.w3.org/XML)

[2] www.trustcenter.de.

[3] Vgl. dazu die Themenseite des Bundesamts für Justiz «Bundesgesetz über die elektronische Signatur», www.ofj.admin.ch/themen/digsig/intro-d.htm, und die Themenseite des Bundesamts für Kommunikation «Elektronische Signatur», www.bakom.ch/de/telekommunikation/internet/digsig/index.html.

[4] Vgl. www.microsoft.com/windowsserver2003/technologies/rightsmgmt.

[5] Dokumentenräume sind programmdisjunkt, wenn es zu jedem digitalen Dokument genau ein Programm gibt, mit dem es bearbeitet werden kann, und für das es entsprechend auch eine gültige Eingabe darstellt.

[5] Vgl. dazu die SDA-Meldung «Gefälschte Bussentabelle im Umlauf», 25. September 2004, 09:50, NZZ Online, www.nzz.ch/2004/09/24/vm/page-newzzDZIG33F9-12.html.

Rechtsgebiet:	Rechtsinformatik
Erschienen in:	Jusletter 8. November 2004
Zitiervorschlag:	Rolf Oppliger, Digitale Dokumente – Alte und neue Herausforderungen sowie Lösungsansätze, in: Jusletter 8. November 2004
Internetadresse:	http://www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=3416