Eva Schmid

Theorie und Praxis des Dokumentenbeweises im Internetzeitalter

Zusammenfassung des französischsprachigen Referates von Jean-François Blanchette, an der Tagung für Informatik und Recht 2004 in Bern

Mit einem Streifzug durch die kryptologischen Ursprünge der elektronischen Signatur und Verschlüsselungstechniken legte Ass. Prof. Dr. Jean-François Blanchette anhand von EU-Richtlinien sowie insbesondere auch anhand des französischen Zivilrechts die Komplexität der Beweisführung mittels elektronischer Dokumente dar. Nebst der Frage, wie bzw. durch wen die Authentizität der digitalen Signatur bestätigt werden kann und von welcher Lebensdauer diese überhaupt ist, wurden abschliessend die InterPARES-Prinzipien erläutert.

[Rz 1] Der Ursprung der elektronischen/digitalen Signatur liegt in der Wissenschaft der Kryptologie, die bereits Geheimdiensten wie der National Security Agency (NSA), Diplomaten und Militär eine vertrauliche Kommunikations- und Übermittlungstechnik bot. Im Jahre 1976, nachdem durch das vermehrte Sicherheitsbedürfnis der Banken eine zivile Kryptographie aufgekommen war, stellten Diffie und Hellmann [1] als Äquivalent zur handschriftlichen Signatur das Konzept der «Kryptographie mittels öffentlichem Schlüssel» zur Verfügung. Dieses Konzept funktioniert so, dass jeder Anwender pro Netz über zwei Schlüssel verfügt, nämlich einen privaten, den er geheim hält, und einen öffentlichen, der in einem Verzeichnis allen Netzanwendern zugänglich ist. Ab Mitte der 1990er-Jahre begannen etliche internationale Institutionen, u.a. CNUDCI [2], ABA[3] und OECD[4], ihre Zugänge und elektronischen Signaturen zu kodieren.

[Rz 2] Zwischen 1996 und 2000 wurden dann in vielen Ländern neue Rechtsgrundlagen über die elektronische Signatur geschaffen und die verfahrensrechtlichen Normen hinsichtlich des elektronischen Dokumentenbeweises revidiert. Für den EU-Raum ausschlaggebend ist die EU-Richtlinie aus dem Jahr 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen[5], welche die Mitglied-Staaten dazu verpflichtet hat, ihre Gesetzgebung insbesondere bezüglich des Urkundenbeweises entsprechend zu revidieren. Ferner wird die Beweiskraft der elektronischen Signatur in die «einfache elektronische Signatur» und in die «fortgeschrittene elektronische Signatur» unterteilt, wobei bei Letzterer jede nachträgliche Modifizierung nachvollziehbar und entschlüsselbar sein muss.

[Rz 3] Das französische Beweisrecht [6] anerkannte bis zum Jahr 1980 ausschliesslich Papier-Schriftstücke als Beweismittel; hierarchisch an erster Stelle stand die öffentliche Urkunde, danach die Privaturkunde sowie schliesslich die übrigen Schriftstücke, die nur als Indizien anerkannt wurden. Die Revision von 1980 entsprach den Bedürfnissen der Industrie, der Banken und Versicherungen und brachte die Anerkennung des Mikrofilms als erstes Nicht-Papier-Beweismittel. Die im Jahre 2000 durchgeführte Reform brachte einerseits eine klare Definition der Schriftlichkeit, andererseits die verfahrensrechtlichen Zulassungskriterien für elektronische Schriftstücke als Beweismittel und damit eine Gleichstellung der Beweiskraft mit jener von Papier-Schriftstücken. Im Weiteren wurde die EU-Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen in Frankreich mit einem neuen Gesetz, Gesetz Nr. 2000-230 vom 13. März 2000 [7], umgesetzt. Die französischen Notare gründeten daraufhin das «Réseau électronique notarial (R.E.AL)[8]», eine Intranet-Plattform für französische Notare und ihre Mitarbeitenden. R.E.AL funktioniert mit einem kreditkartenähnlichen Ausweis, über den Identifikation und Sicherung der Daten sowie der Austausch mit anderen Notaren und auch der Zugang zu Datenbanken, z.B. zum Zentralregister der letztwilligen Verfügungen, ermöglicht wird.

[Rz 4] Um die nicht gesetzlich festgelegte Aufbewahrung bzw. das Nicht-Vorhandensein von Fristen betreffend elektronische Urkunden zu regeln, hat die französische Regierung zwei Arbeitsgruppen mit der Klärung der entsprechenden Aufbewahrungsmodalitäten beauftragt. Unter anderem unterstreichen diese Arbeitsgruppen die Problematik der Leserlichkeit des jeweiligen Dokuments im Zusammenhang mit der Beibehaltung seines Wertes als Beweismittel. Gerade wegen der rapiden Weiterentwicklung der Informatik-Programme könnten ältere elektronische Dokumente eines Tages mit den aktuellen Programmen nicht mehr lesbar sein, was mitunter auch den Umgang mit der elektronischen Signatur erschwert. Wenngleich diese nicht modifizierbar sein soll, müssten Computerprogramme darauf eingerichtet sein, ältere elektronische Signaturen lesbar anzuzeigen. Die im Jahre 1999 initiierte Reform des

französischen Beweisrechts nimmt sich dieser Problematik allerdings nicht an.

[Rz 5] InterPARES[9] ist ein Forschungsprojekt, das Vertreter von Nationalarchiven von vier Kontinenten vereint und sich mit der Problematik der Aufbewahrung von elektronischen Urkunden befasst. Im Jahr 2004 hat InterPARES Prinzipien zur Überprüfung der Praktikabilität der bestehenden Normen und Gesetze im Zusammenhang mit elektronischen Urkunden vorgeschlagen. Jede Organisation sollte anhand dieser Prinzipien die Langlebigkeit und Echtheit seiner elektronischen Urkunden überprüfen. Die beste Garantie der Echtheit ist im Übrigen nicht technologischer Natur, sondern wie innerhalb eines Verwaltungssystems, die Rolle des Archivars als Wärter des investierten Vertrauens.

[Rz 6] «Wenn Sie glauben, die Kryptographie könne Ihre Probleme lösen, dann verstehen Sie weder die Kryptographie, noch Ihre Probleme» – so abschliessend ein Zitat nach den Kryptographen Ellison und Needham.

Die Autorin, Eva K. Schmid, ist Studentin der Rechtswissenschaften und dipl. Handelskauffrau. Nebst ihrem Studium ist sie einerseits als Lektorin juristischer Publikationen, andererseits innerhalb der Bundesverwaltung tätig.

Der vorliegende Beitrag ist eine Zusammenfassung des französischsprachigen Referates von Ass. Prof. Dr. Jean-François Blanchette, an der Tagung für Informatik und Recht 2004: Jean-François Blanchette, Théorie et pratique de la preuve documentaire à l´ère de l´électronique, in: Jusletter 8. November 2004.

---

[1] Der 1976 von Whitfield Diffie und Martin E. Hellmann entwickelte Diffie-Hellmann-Algorithmus ist der erste Public-Key-Algorithmus, der für die Schlüsselvereinbarung über einen unsicheren Kanal verwendet wird, und somit stellte das Verfahren eine Revolution in der Kryptographie dar, vgl. u.a. auch auf der Homepage des Lehrstuhls für Datenverarbeitung der Universität Bochum: http://www.etdv.ruhr-uni-bochum.de/dv/lehre/seminar/krypto/sld013.htm

[2] Commission des Nations Unies pour le droit commercial international (CNUDCI), vgl. unter http://www.uncitral.org/

[3] American Bar Association (ABA), vgl. unter http://www.abanet.org/

[4] Organisation de coopération et de développement économiques (OCDE), vgl. unter http://www.oecd.org

[5] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, vgl. unter http://europa.eu.int/eur-lex/de/, in: Amtsblatt Nr. L 013 vom 19/01/2000 S. 0012 – 0020.

[6] Code civil français Art. 1341 ff. (De la preuve testimoniale), vgl. unter http://www.legifrance.gouv.fr/WAspad/ListeCodes

[7] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information relative à la signature électronique, vgl. unter http://www.legifrance.gouv.fr/WAspad/RechercheSimpleLegi.jsp

[8] Réseau électronique notarial (R.É.AL), vgl. unter http://notaires-v.iside.net/art.php?cID=11&nID=524

[9] International Research on Permanent Authentic Records in Electronic Systems (InterPARES), für weitere Informationen vgl. unter http://www.interpares.org/

Rechtsgebiet: Informatik und Recht
Erschienen in: Jusletter 8. November 2004
Zitiervorschlag: Eva Schmid, Theorie und Praxis des Dokumentenbeweises im Internetzeitalter, in: Jusletter 8. November 2004
Internetadresse: http://www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=3514