Heiko Heibel

Die digitale Signatur

Rechtliche, informationstechnische und ökonomische Aspekte einer digitalen Verifizierung nach dem Gesetz über Rahmenbedingungen für elektronische Signaturen

Diplomarbeit

Diplom.de

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlages. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Copyright © 2003 Diplom.de
ISBN: 9783832470678

https://www.diplom.de/document/222386

Heiko Heibel

Die digitale Signatur

Rechtliche, informationstechnische und ökonomische Aspekte einer digitalen Verifizierung nach dem Gesetz über Rahmenbedingungen für elektronische Signaturen

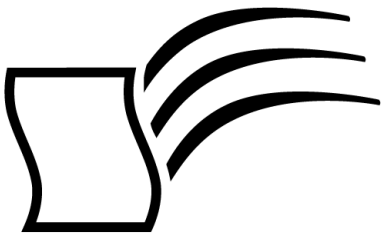
Diplom.de

Heiko Heibel

Die digitale Signatur

Rechtliche, informationstechnische und ökonomische Aspekte einer digitalen Verifizierung nach dem Gesetz über Rahmenbedingungen für elektronische Signaturen

Diplomarbeit
Bergische Universität - Gesamthochschule Wuppertal
Fachbereich Wirtschaftswissenschaften
Abgabe Juni 2003



Diplom.de

Diplomica GmbH
Hermannstal 119k
22119 Hamburg

Fon: 040 / 655 99 20
Fax: 040 / 655 99 222

agentur@diplom.de
www.diplom.de

ID 7067
Heibel, Heiko: Die digitale Signatur - Rechtliche, informationstechnische und ökonomische Aspekte einer digitalen Verifizierung nach dem Gesetz über Rahmenbedingungen für elektronische Signaturen
Hamburg: Diplomica GmbH, 2003
Zugl.: Bergische Universität - Gesamthochschule Wuppertal, Universität - Gesamthochschule, Diplomarbeit, 2003

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden, und die Diplomarbeiten Agentur, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

Diplomica GmbH
http://www.diplom.de, Hamburg 2003
Printed in Germany

Zusammenfassung

Die Informationstechnologie weist neben zahlreichen betriebswirtschaftlichen Anwendungsmöglichkeiten, ebenfalls verschiedene Risiken auf. Diese zeigen sich insbesondere in der Flüchtig- und Manipulierbarkeit elektronischer Daten. Nach verschiedenen Einschätzungen stellt derzeit z. B. das in einem gerichtlichen Verfahren kaum nachweisbare Zustandekommen elektronisch geschlossener Verträge, eine erhebliche Behinderung des elektronischen Handels dar.

Durch verschiedene Rechtsanpassungen auf europäischer und nationaler Ebene wurde ein elektronischer Signaturtyp geschaffen, der in Analogie zur eigenhändigen Unterschrift, die Integrität und Authentizität von elektronischen Daten ermöglichen soll. Die Regelungen des Signaturgesetzes beschränken sich hierbei im wesentlichen auf infrastrukturelle und informationstechnische Spezifikationen. Durch Formanpassungen in verschiedenen Bereichen des Privat- und öffentlichen Rechts wurde die ***qualifizierte elektronische Signatur*** teilweise zu einem vollwertigen rechtlichen Substitut der eigenhändigen Unterschrift. Die Regelung zur dauerhaften Überprüfbarkeit sowie die Beweiswirkung ist jedoch nicht durchgängig stringent geregelt.

Als Basiskonzept dient die Public-Key-Kryptographie unter Einbeziehung einer vertrauenswürdigen Instanz. Hierdurch ist die qualifizierte elektronische Signatur im Vergleich zur Unterschrift deutlich fälschungssicherer. Die Sicherheit der verwendeten Verfahren und Algorithmen ist unter Verwendung entsprechender Parameter sehr hoch. Im Vergleich zu den ausgeprägten Anforderungen an Infrastrukturanbieter existieren im Bereich der Anwender dagegn kaum Sicherheitsbestimmungen, wodurch sich gerade private Nutzer einem gewissen Bedrohungspotential durch sogenannte Trojaner ausgesetzt sehen müssen.

Als Ursache für die fehlende Durchsetzung der *qualifizierten elektronischen Signatur* sind schließlich nicht allein die sich gegenseitig bedingenden Faktoren wie konkurrierende Signaturverfahren, hohe Kosten der qualifizierten Signatur und mangelnde Kommunikationspartner zu identifizieren. Vielmehr zeichnen sich in einigen Szenarien jenseits der Prozessoptimierung und der reinen Kostenerwägung keine ausreichenden Nutzenpotentiale für ihre Akteure ab: Zur eindeutigen Identifikation des Gegenübers sind de facto immer noch zusätzliche Mechanismen erforderlich; die elektronische Mobilität von Kunden kann nach Marketinggesichtspunkten des einzelnen Unternehmens als durchaus kontraproduktiv gesehen werden; gesetzlich manifestierte Interaktionsregeln des elektronischen Geschäftsverkehrs und implizite Sicherungsmechanismen bieten u. U. eine deutlich höhere Praktikabilität.

Inhaltsverzeichnis

1 Vorbemerkungen 5

2 Rechtliche Aspekte der Signatur 10

2.1 Rechtliche Grundlagen 10

2.1.1 Richtlinie der Europäischen Union 10

2.1.2 Deutscher Gesetzgeber 11

2.2 Anforderungen an eine qualifizierte elektronische Signatur 15

2.2.1 Definition und Abgrenzung 15

2.2.2 Produkte für qualifizierte elektronische Signaturen 16

2.2.2.1 Sichere Signaturerstellungseinheiten 17

2.2.2.2 Signaturanwendungskomponenten 18

2.2.2.3 Technische Komponenten für Zertifizierungsdienste 20

2.2.3 Qualifizierte Zertifikate und Wurzelzertifikate 20

2.2.4 Dynamische Aspekte des Sicherheitsgehalts von qualifizierten elektronischen Signaturen 24

2.3 Die qualifizierte elektronische Signatur als „Substitut“ 28

2.3.1 Privatrechtsbereich 28

2.3.2 Öffentlich-rechtlicher Bereich 30

2.4 Besonderheiten im Zusammenhang mit akkreditierten Zertifizierungsdiensteanbietern 32

3 Die informationstechnische Realisierung 35

3.1 Das kryptographische Konzept 35

3.2 Das Funktionsprinzip des Signierens und Verifizierens 38

3.2.1 Das Signieren 38

3.2.2 Das Verifizieren 39

3.3 Geeignete Kryptoalgorithmen und Sicherheitsparameter 41

3.3.1 Hashfunktionen 41

3.3.2 Signaturalgorithmen 42

3.3.2.1 Das RSA-Verfahren 42

3.3.2.2 DSA und DSA-Varianten (ECC) 44

3.3.3 Gefahrenpunkte und Schwachstellen der Kryptosysteme 45

3.4 Produkte und ihre Anwendung 47

3.4.1 Die Signatur-Produkte des Anwenders 47

3.4.1.1 Sichere Signaturerstellungseinheiten 48

3.4.1.2 Signaturanwendungskomponenten 49

3.4.2 Die Gefahrenpotentiale sogenannter Trojaner für die Signaturerstellung 52

3.5 Die Public-Key-Infrastruktur 55

3.5.1 Interoperabilität 55

3.5.2 Zertifizierungs-Infrastruktur 57

3.5.3 Gültigkeitsmodell 59

4 Ökonomische Gegenwart und Perspektiven 62
4.1 Die Ökonomische Vertragstheorie 64
4.1.1 Implizite Verträge 65
4.1.2 Relationale Verträge 65
4.2 Die Stellung von Verbraucher und Bürger 67
4.2.1 Kauf-, Dienstleistungs-, Reise- und Mietverträge 67
4.2.1.1 Fernabsatzverträge, Internetauktionen 67
4.2.1.2 Reise- und Mietverträge 73
4.2.2 Finanz- und Versicherungsgeschäfte 75
4.2.2.1 Finanzgeschäfte und –transaktionen 75
4.2.2.2 Versicherungsgeschäfte 78
4.2.3 „Behördengänge“ 79
4.3 Unternehmerische Potentiale der qualifizierten elektronischen Signatur 82
4.3.1 Grundsätzliche ökonomische Potentiale 82
4.3.2 Besondere Aspekte im E-Commerce 82
4.4 E-Government 84
5 Fazit 86
6 Anhang 88
7 Verzeichnisse 95
7.1 Literaturverzeichnis 95
7.2 Internetquellen 99
7.3 Verwendete Software 100
7.4 Abbildungs- und Tabellenverzeichnis 101

1 Vorbemerkungen

Die Kommunikation der vergangenen Jahre zeichnet sich durch eine deutliche Verlagerung weg von den traditionellen Medien (z. B. Brief, Telefon) aus. Den Inhalten der in elektronischer Form übermittelten Daten und Informationen kommt dabei eine immer stärkere ökonomische Bedeutung zu. Mit dem Netz der *‚Society for Worldwide Interbank Financial Telecommunication'* (S.W.I.F.T.) werden z. B. täglich Transaktionen im Wert von schätzungsweise über 6 Billionen US-Dollar durchgeführt.[1] Dies stellt gut ein Fünftel des weltweiten (jährlichen) Bruttosozialproduktes[2] dar. Mit der elektronischen Kommunikation hat sich im Bereich der offenen Netze das Internet als eine wesentliche Infrastrukturkomponente, sowohl auf internationaler wie auch auf nationaler Ebene, herausgebildet. In Deutschland nutzt inzwischen nahezu jeder zweite Erwachsene das Internet und die Zahl wächst trotz abgeschwächter Interneteuphorie kontinuierlich.[3] Im ersten Quartal 2002 lagen die deutschen Haushalte, die über einen Internetzugang verfügten, mit einem Anteil von 43% über dem EU-Durchschnitt (40%) und auch die deutschen Unternehmen (verarbeitende Gewerbe, Handel und weitere Dienstleistungsbereiche) wiesen mit 62% ein hohes Niveau auf.[4] *„Über die Zukunft dieses Mediums bestehen (...) weitgehend übereinstimmende Auffassungen. Bereits jetzt haben sich in den Bereichen eBusiness und eGovernment in einem historisch sehr kurzem Zeitraum zahlreiche unterschiedliche Anwendungen entwickelt, die auf der Internettechnologie aufsetzen, z. B. Internet-Banking, eCommerce mit Zahlungstransaktionen, Virtuelle Rathäuser, Online-Wahlen, Online-Auktionen, Dateiaustausch per FTP oder eMail."*[5] In deutschen Unternehmen ist die E-Mail inzwischen zu einem alltäglichen Kommunikationswerkzeug geworden. Umfragen zu Folge liegt das tägliche E-Mail-Aufkommen bei durchschnittlich 26 Mails und über die Hälfte aller Anwender gehen von einer Intensivierung ihrer E-Mail-Nutzung innerhalb des nächsten Jahres aus.[6]

Die Informationstechnologie (IT), als Basistechnologie elektronisch digitaler Kommunikation, ermöglicht eine Vielzahl neuer Dienstleistungsangebote und die Chance verschiedenster Prozessoptimierungen bzw. –neugestaltungen.[7] Elektronische Kommunikation im weitesten Sinne ist inzwischen ebenfalls als ein bedeutender Faktor zur Beeinflussung der Transaktions-

---

1 vgl. z. B. http://www.swift.com/index.cfm?item_id=3184
2 vgl. z. B. http://www.diw.de/deutsch/publikationen/wochenberichte/docs/02-37-1.html
3 vgl. z. B. van Eimeren (2002, S. 346), @facts (2002, S. 5), @facts extra (2002, S. 6), http://www.ard-werbung.de/_mp/fach/200208_01.phtml, http://www.emind.emnid.de/downloads/studien/20021171GO2002Germany.pdf
4 vgl. z. B. http://www.destatis.de/presse/deutsch/pm2003/p0510024.htm
5 BMWT/KPMG (2001, S. 8)
6 vgl. SofTrust Consulting (2002)
7 vgl. z. B. Stähler (2001)

kosten[8] erkannt worden. Neben den unterschiedlichen Verbesserungen bergen die neuen Technologien mit ihren betriebswirtschaftlichen Anwendungsmöglichkeiten, aber ebenfalls zahlreiche Risiken und Unzulänglichkeiten in sich. Hier ist z. B. an die ***Unsicherheit bezüglich Urheberschaft und Unverfälschtheit von Daten und Informationen*** (vgl. Abbildung 1) gerade in offenen Netzen zu denken (Internet) – aber auch einem weitestgehend nur eingeschränktem Nutzerkreis zugängliche Bereiche können bei hinreichend großer Anwenderzahl betroffen sein (Intranet, Extranet). Diesen Risiken kommt insbesondere dann eine starke Bedeutung zu, wenn ***rechtlich und ökonomisch relevante Willenserklärungen*** Gegenstand von Informationen sind bzw. sein sollen. Eine erhebliche Behinderung des elektronischen Handels über das Internet stellt nach verschiedenen Einschätzungen derzeit immer noch das in einem gerichtlichen Verfahren kaum beweisbare Zustandekommen von wirksamen Verträgen z. B. durch E-Mail dar.[9] Das Kernproblem liegt also nicht in der formalen Frage einer Wirksamkeit elektronischer Willenserklärungen, als vielmehr in dem Umstand der Flüchtig- und Manipulierbarkeit elektronischer Daten.[10]

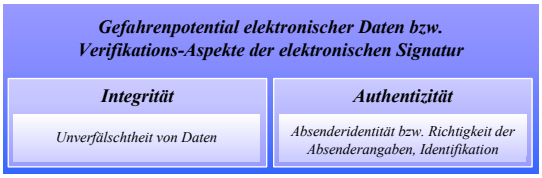


Abbildung 1: Mögliche Gefahrenpotentiale bei Daten in elektronischer Form und damit verbundene Aspekte für das elektronische Signieren

Mit dem *Informations- und Kommunikationsdienste-Gesetz*[11] (IuKDG) vom 22. Juli 1997 hat sich der deutsche Gesetzgeber in diesem Zusammenhang wesentlicher Sicherheitsaspekte angenommen. Das Gesetz zur digitalen Signatur von 1997 (Art. 3 IuKDG) traf hieraufhin erstmalig Regelungen für das digitale Signieren (SigG 1997). Durch die *Richtlinie 1999/93/EG*[12] (RL1999/93/EG) des Europäischen Parlaments und Rates wurde im Dezember 1999 ein einheitlicher europäischer Rechtsrahmen für elektronische Signaturen geschaffen, der eine Anpassung der deutschen Vorschriften erforderlich machte – mit dem *Gesetz über Rahmenbedingungen für elektronische Signaturen*[13] (SigG 2001) wurde das bis dahin einschlägige SigG 1997 abgelöst.

Die digitale bzw. elektronische Signatur kann allerdings nur dann zu einer nachhaltigen Anwendung kommen, wenn die verschiedenen Rechtsnormen neben der bisherigen Schriftform auch die elektronische Form anerkennen, d. h. die elektronische Abbildung von Dokumenten (z. B. als Träger von Willenserklärungen) muss zusammen mit ihrer elektronischen Übertragung Berücksichtigung und Rechtswirksamkeit erfahren.[14] Durch das *Gesetz zur Anpassung*

---

8 vgl. z. B. Richter (1999)
9 vgl. z. B. Armgardt (2001)
10 vgl. z. B. Sanner (2001)
11 BGBl. I 1997, S. 1870 ff.
12 ABl. EG Nr. 13 v. 19.1.2000, S. 14 ff.
13 BGBl. I 2001, S. 876 ff.
14 vgl. z. B. Roßnagel (2002, S. 13)