Elektronische Signaturen in der VR China

Simon Werthwein[*]

I. Einleitung

Das „Gesetz der VR China über elektronische Signaturen“[2] (SigG) wurde auf der 11. Sitzung des Ständigen Ausschusses des 10. Nationalen Volkskongresses am 28.08.2004 verabschiedet, durch Dekret Nr. 18 des Präsidenten HU Jintao bekannt gemacht und ist am 01.04.2005 in Kraft getreten. Bis zu diesem Zeitpunkt waren elektronische Signaturen in der VR China nur uneinheitlich und in örtlich und sachlich eng begrenzten Bereichen geregelt.[3]

Nach einer allgemeinen Einführung zur elektronischen Signatur (II.) sollen die denkbaren Modelle gesetzlicher Regelung anhand einiger Beispiele vorgestellt werden (III.). Sodann wird die Rechtslage in der VR China vor und nach dem Inkrafttreten des SigG im Einzelnen dargestellt (IV. und V.). Ein kurzer Ausblick (VI.) beschließt den Beitrag.

II. Elektronische Signatur

1. Problemstellung

Elektronische Kommunikation ist aus dem heutigen Geschäftsverkehr nicht mehr wegzudenken. Während das Telefon aufgrund der Flüchtigkeit des gesprochenen Wortes kaum zur Übermittlung rechtserheblicher Erklärungen von größerer Tragweite geeignet ist, eröffnet die Verbreitung von Fax und E-Mail immerhin die Möglichkeit, in ähnlicher Geschwindigkeit wie am Telefon ohne persönlichen Kontakt zwischen den Parteien Willenserklärungen auszutauschen, die als Papier- oder als elektronisches Dokument archivierbar sind. Weder Fax noch E-Mail können jedoch eine Originalunterschrift des Erklärenden enthalten, so dass der Empfänger über die Authentizität, also darüber, ob die empfangene Erklärung tatsächlich vom angegebenen Urheber stammt, im Ungewissen bleibt. Es kann so lediglich die Textform,[4] nicht aber die in bestimmten Fällen erforderliche Schriftform eingehalten werden. Insbesondere bei der E-Mail ist außerdem die inhaltliche Integrität zweifelhaft, da diese Form der elektronischen Kommunikation stets dem Verdacht der Manipulation entweder auf dem Weg vom Erklärenden zum Empfänger durch Dritte oder nach Empfang durch den Empfänger selbst ausgesetzt ist. Die genannten Mängel sollen in Fällen der Übermittlung elektronischer Dokumente per E-Mail durch die elektronische Signatur behoben werden.

2. Begriffe und Funktionen

a) Elektronische Signatur

Üblicherweise wird die elektronische Signatur definiert als „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“. [5] Diesen Tatbestand erfüllt bereits die bloße Namensangabe unter einer E-Mail.[6] Dies löst allerdings die oben dargestellten Probleme nicht.

b) Fortgeschrittene elektronische Signatur

Vielmehr muss dazu eine elektronische Signatur verwendet werden, die mindestens die folgenden Voraussetzungen erfüllt:

- Ausschließliche Zuordnung zum Unterzeichner;

- Ermöglichung der Identifizierung des Unterzeichners;

- Erstellung mit Mitteln, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;

- Verknüpfung mit den signierten Daten in einer Weise, die eine nachträgliche Veränderung der Daten erkennbar macht.

Die ersten drei genannten Merkmale dienen der Authentifizierung des signierten elektronischen Dokuments, während das letztgenannte Merkmal die Integrität des elektronischen Dokuments sicherstellt. Elektronische Signaturen, die die oben genannten Voraussetzungen erfüllen, werden auch

[*] Praktikant am Institut.

[2] Siehe die chinesisch-deutsche Fassung des Gesetzes in diesem Heft.

[3] Vgl. dazu unten IV.

[4] Vgl. § 126 b BGB.

[5] Siehe Art. 2 Nr. 1 der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (RLeS); diese Definition ähnelt stark derjenigen in Art. 2 lit. a des „UNCITRAL Model Law on Electronic Signatures“ aus dem Jahr 2001 (dazu unten Fn. 23). Ähnlich auch Section 106 (5) des „Electronic Signatures in Global and National Commerce Act“ der USA vom 08.06.2000, in Kraft getreten am 01.10.2000 (zitiert nach *Ivo Geis*, Die elektronische Signatur: Eine internationale Architektur der Identifizierung im E-Commerce, in: MultiMedia und Recht 2000, S. 673).

[6] *Uwe Blaurock/Jürgen Adam*, Elektronische Signatur und europäisches Privatrecht, in: Zeitschrift für Europäisches Privatrecht 2001, S. 95.

als „fortgeschrittene elektronische Signaturen" bezeichnet.[7]

3. Technische Umsetzung

Die Benennung der Funktionen, die eine elektronische Signatur erfüllen muss, sagt noch nichts über die technische Realisierung dieser Funktionen. Es stehen im Wesentlichen folgende Möglichkeiten zur Auswahl:

a) Biometrische Verfahren

Biometrische Verfahren basieren auf der Messung unverwechselbarer biologischer Eigenschaften wie des Fingerabdrucks.[8] Möglich ist unter anderem auch die Erfassung von Augenbewegungen oder die der Schreibgeschwindigkeit, der Strichreihenfolge und -richtung sowie ggf. des Anpressdrucks beim manuellen Verfertigen einer herkömmlichen Unterschrift.[9] Ein Vorteil dieser Verfahren ist, dass die zugrunde liegenden Merkmale auf natürliche Weise ausschließlich dem Unterzeichner zugeordnet sind und schwerlich unter die Kontrolle Unbefugter gelangen können, also hinsichtlich der Authentifizierungsfunktion kaum Wünsche offen bleiben. Die Sicherung der Integrität des signierten Dokuments hängt wie auch bei den sogleich anzusprechenden kryptographischen Verfahren von der Art und Weise der Verknüpfung der Signatur mit den signierten Daten ab.

b) Kryptographische Verfahren

aa) Symmetrische Kryptographie

Die symmetrische Kryptographie beruht auf einem „privaten Schlüssel", der beiden Parteien zur Verfügung steht (Shared Private Key-Verfahren). Ein solcher privater Schlüssel kann beispielsweise eine PIN (personal identification number) sein, wie sie vielfach an Bankautomaten zum Einsatz kommt.[10] Bei diesem System benutzen beide Parteien denselben Schlüssel zur Ver- und Entschlüsselung der Nachricht. Problematisch ist, dass ein per E-Mail übermittelter privater Schlüssel leicht von Unbefugten abgefangen werden kann; zudem müssen beide Parteien darauf vertrauen, dass die jeweils andere Partei den privaten Schlüssel nicht an Unbefugte weitergibt.[11] Die symmetrische Kryptographie ist daher für Zwecke der elektronischen Signierung wenig geeignet.

bb) Asymmetrische Kryptographie[12]

Dieses Verfahren beruht auf einem Paar einander mathematisch eindeutig zugeordneter Schlüssel, dem privaten und dem öffentlichen Schlüssel (Public Key-Verfahren). Der Autor der Nachricht verschlüsselt diese mit Hilfe seines nur ihm zugänglichen privaten Schlüssels, indem die Daten des elektronischen Dokuments nach einem bestimmten technischen Verfahren zu einem so genannten Hash-Code[13] komprimiert werden, der dann mit dem privaten Schlüssel verknüpft wird.[14] Sowohl das signierte Komprimat (z. B. eine Zeile) als auch das unverschlüsselte elektronische Dokument (z. B. 20 Seiten) werden dem Empfänger übermittelt.[15] Dieser erhält außerdem entweder vom Absender der Nachricht oder von einem Dritten den zu dem privaten Schlüssel gehörigen öffentlichen Schlüssel, mit dem er den Hash-Code dekomprimieren kann.[16] Stimmen das unverschlüsselte und das entschlüsselte Dokument überein, so weiß der Empfänger, dass ihn die Nachricht des Absenders unverfälscht erreicht hat und dass die Nachricht tatsächlich vom Inhaber des privaten Schlüssels stammt, dem der von ihm zur Dekomprimierung verwendete öffentliche Schlüssel zugeordnet ist. Der private Schlüssel bleibt also geheim, während der öffentliche Schlüssel ohne großen Aufwand und ohne Risiko öffentlich abrufbar gemacht oder auf andere Weise an den Empfänger übermittelt werden kann.[17] Aus diesem Grund eignet sich dieses Verfahren gut für die Zwecke der elektronischen Signierung. Praktisch wird dieses Verfahren derzeit so durchgeführt, dass der private Schlüssel durch eine PIN geschützt gemeinsam mit der gesamten manipulationsgeschützten Signiertechnik auf einer Chipkarte gespeichert wird, zu deren Verwendung ein PC mit einer speziellen Software und einem Chipkartenlesegerät benötigt wird.[18]

Anders als bei biometrischen Verfahren ist aber hier der private Schlüssel (und bei asymmetrischer

---

[7] Vgl. Art. 2 Nr. 2 RLeS (Fn. 4).
[8] *Uwe Blaurock/Jürgen Adam* (Fn. 5), S. 94.
[9] *Ian A. Rambarran*, I Accept, But Do They? The Need for Electronic Signature Legislation on Mainland China, in: The Transnational Lawyer 2002, S. 408.
[10] *Ian A. Rambarran* (Fn. 8), S. 410.
[11] *Ian A. Rambarran* (Fn. 8), S. 411.
[12] Eine detailliertere Darstellung ist zu finden in: Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001), Ziff. 35 ff. (dazu unten Fn. 23).
[13] Engl. hash: Durcheinander, Kuddelmuddel; nähere Erläuterungen in: Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001), Ziff. 40 (dazu unten Fn. 23).
[14] *Ulrich Noack*, Elektronische Signatur, elektronische Form und Textform, in: Deutsches Steuerrecht 2001, S. 1894.
[15] *Wendelin Bieser*, Das neue Signaturgesetz – Die digitale Signatur im europäischen und internationalen Kontext, in: Deutsches Steuerrecht 2001, S. 27.
[16] *Wendelin Bieser* (Fn. 14), S. 27.
[17] *Ian A. Rambarran* (Fn. 8), S. 411.
[18] *Wendelin Bieser* (Fn. 14), S. 27.

Kryptographie der außerdem benötigte öffentliche Schlüssel) nicht auf natürliche Weise einer Person zugeordnet. Vielmehr muss diese Zuordnung von einer dritten Partei, einer so genannten Zertifizierungsstelle, vorgenommen werden. Diese weist dem Teilnehmer ein Schlüsselpaar zu und stellt ihm ein elektronisches Zertifikat aus, das die Zuordnung des Schlüsselpaares zu seiner Person bestätigt. Dieses Zertifikat kann neben den oben genannten Daten auf der Chipkarte gespeichert werden und neben der in verschlüsselter und unverschlüsselter Form versendeten Nachricht dem Empfänger übermittelt werden. Über dieses Zertifikat kann der Empfänger den öffentlichen Schlüssel bei der Zertifizierungsstelle abrufen. Die Zertifizierungsstelle ermöglicht über den öffentlichen Schlüssel also die Prüfung der Integrität der Nachricht sowie über das Zertifikat in Verbindung mit dem öffentlichen Schlüssel die Überprüfung der Authentizität.

Die Notwendigkeit der Beteiligung einer Zertifizierungsstelle beruht auf der Definition eines weiteren Signaturstandards im deutschen Signaturgesetz [19] (deutsches SigG), nämlich der „qualifizierten elektronischen Signatur" gem. § 2 Nr. 3. Nach dieser Vorschrift muss eine solche qualifizierte elektronische Signatur die Voraussetzungen einer fortgeschrittenen elektronischen Signatur (siehe dazu oben II.2.b)) erfüllen und darüber hinaus unter anderem auf einem Zertifikat beruhen, das ein Zertifizierungsdiensteanbieter ausgestellt hat, der mindestens die Anforderungen nach den §§ 4 bis 14 oder § 23 des deutschen SigG und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 des deutschen SigG erfüllt. [20] Elektronische Signaturen, die mit Hilfe asymmetrischer Kryptographie erzeugt werden, bezeichnet man in Abgrenzung zu sonstigen elektronischen Signaturen auch als digitale Signaturen.[21]

III. Möglichkeiten gesetzlicher Regelung

1. Technologieneutral oder technologiespezifisch

Die zentrale Frage an jede gesetzliche Regelung in Bezug auf elektronische Signaturen ist, ob die Regelung technologiespezifisch oder technologieneutral ist. Technologiespezifische Regelungen knüpfen die rechtliche Beachtlichkeit elektronischer Signaturen daran, dass eine bestimmte gesetzlich vorgeschriebene Technologie eingesetzt wird, wie beispielsweise das Public Key-Verfahren. Technologieneutrale Regelungen [22] dagegen legen keine bestimmte Technologie fest und überlassen die Antwort auf die sich im Einzelfall stellende Frage nach der Wirksamkeit einer elektronisch signierten Erklärung den Gerichten. Schließlich gibt es noch den Mittelweg einer zweistufigen Regelung: es bleibt grundsätzlich dem Rechtsverkehr überlassen, welche Technologie eingesetzt wird, jedoch wird ein bestimmtes Verfahren oder eine Gruppe von Verfahren privilegiert, z. B. in beweisrechtlicher Hinsicht.

2. Beispiele gesetzgeberischer Ansätze

a) Das UNCITRAL Model Law on Electronic Signatures

Die United Nations Commission on International Trade Law (UNCITRAL) wurde 1966 gegründet und hat die Aufgabe, die Harmonisierung und Vereinheitlichung des Rechts des internationalen Handels voranzutreiben; unter den 60 Mitgliedsstaaten befindet sich auch die VR China. [23] Das „UNCITRAL Model Law on Electronic Signatures" (MLES) wurde gemeinsam mit einem im gleichen Dokument enthaltenen „Guide to Enactment" (Guide MLES) veröffentlicht.[24] Das MLES und der Guide MLES sollen den nationalen Gesetzgebern beim Erlass entsprechender Gesetze Hilfestellung bieten; die im Guide enthaltenen Kommentare sollen darüber hinaus bei der Anwendung solcher Gesetze behilflich sein. [25] Dem MLES liegt ein technologieneutraler Ansatz zugrunde.[26] Jedoch hält Art. 7 Abs. 1 MLES – entsprechend dem Zweck dieses Modellgesetzes, nationalen Gesetzgebern unabhängig vom gewählten Ansatz als Grundlage zu dienen – die Möglichkeit offen, öffentliche oder private Organe zu ermächtigen, bestimmte Formen der elektronischen Signatur als für bestimmte Zwecke ausreichend zu definieren und diese so zu privilegieren.

[19] Gesetz über Rahmenbedingungen für elektronische Signaturen, Bundesgesetzblatt I 2001, S. 876 ff., in Kraft getreten am 22.05.2001.
[20] Vgl. § 2 Nr. 3 a, Nr. 7, Nr. 6, Nr. 8 des deutschen Signaturgesetzes.
[21] Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001), Ziff. 36 (dazu unten Fn. 23); ebenso *Ian A. Rambarran* (Fn. 8), S. 409 und *Wendelin Bieser* (Fn. 14), S. 27 ff.
[22] Näher dazu Guide MLES, Ziff. 107.
[23] Weitere Informationen sind zu finden unter http://www.uncitral.org/english/commiss/geninfo.htm (besucht am 19.05.2005).
[24] General Assembly Resolution 56/80 (2001), abrufbar unter http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf (besucht am 19.05.2005).
[25] Guide MLES, Ziff. 1.
[26] Guide MLES, Ziff. 107.

b) USA

Im Jahr 1995 erließ der Staat Utah ein technologiespezifisches Gesetz, den Utah Digital Signature Act,[27] der nur elektronische Signaturen nach dem Public Key-Verfahren in Verbindung mit einem von einer staatlich autorisierten Zertifizierungsstelle ausgestellten Zertifikat anerkannte.[28] Im gleichen Jahr erging in Kalifornien ein technologieneutrales Gesetz.[29] Auch andere Staaten entfalteten insgesamt uneinheitliche Gesetzgebungsaktivitäten.[30] Zum Zweck der Vereinheitlichung erließen die USA im Jahr 2000 den Electronic Signatures in Global and National Commerce Act,[31] der technologieneutral ausgestaltet ist.[32] Für den technologieneutralen Ansatz spricht, dass das Gesetz auf diese Weise für technische Neuerungen offen bleibt und nicht stur eine eines Tage veraltete Technologie bevorzugt oder gar die Anreize für die Entwicklung besserer Signaturverfahren mindert; außerdem gehen von einer derartigen Regelung weniger Hemmnisse für den internationalen Einsatz elektronischer Signaturen aus.[33] Andererseits wird darauf hingewiesen, dass das Fehlen eines verbindlichen Standards zu Unsicherheiten im Umgang mit elektronischen Signaturen führe, was Justiz und Bürger belaste.[34] Es könne einige Zeit dauern, bis sich im Common Law-System der USA eine klare Linie der Rechtsprechung zu elektronischen Signaturen herausbilde.[35] Es sei zu befürchten, dass diese Probleme die Verbreitung elektronischer Signaturen im Geschäftsverkehr verzögerten.[36]

c) Die Europäische Signaturrichtlinie

Die Europäische Signaturrichtlinie beinhaltet eine zweistufige Regelung. Art. 2 Nr. 1 RLeS enthält zunächst eine technologieneutrale Definition des Begriffs „elektronische Signatur" (vgl. oben II.2.a)). Materiellrechtliche bzw. prozessrechtliche Privilegierungen sind gem. Art. 5 Abs. 1 lit. A bzw. b RLeS aber nur für fortgeschrittene elektronische Signaturen im Sinne des Art. 2 Nr. 2 RLeS (vgl. oben II.2.b)) vorgesehen, die außerdem auf einem qualifizierten Zertifikat (Art. 2 Nr. 10, Nr. 9 RLeS) beruhen und die von einer sicheren Signaturerstellungseinheit (Art. 2 Nr. 6 RLeS) erstellt werden. Damit orientieren sich die Bestimmungen der Richtlinie zur elektronischen Signatur so stark am Verfahren der asymmetrischen Kryptographie, dass hier von Technologieneutralität nicht mehr gesprochen werden kann.[37] Andererseits bestimmt Art. 5 Abs. 2 RLeS, dass einer elektronischen Signatur die rechtliche Wirksamkeit und die Zulässigkeit als Beweismittel im Gerichtsverfahren unter anderem nicht allein deshalb abgesprochen werden darf, weil die Voraussetzungen des Art 5 Abs. 1 RLeS nicht erfüllt sind.[38] Folglich belässt die Richtlinie den Mitgliedstaaten große Freiräume bei der Einführung und Zulassung elektronischer Signaturen und verhindert gleichzeitig die Entstehung uneinheitlicher Standards.[39]

d) Deutschland

In Deutschland sind elektronische Signaturen durch das Signaturgesetz (deutsches SigG) geregelt; neugefasst[40] am 22.05.2001 und geändert[41] am 11.01.2005. Diese technisch-gewerberechtliche Vorschriften[42] sind entsprechend der europäischen Signaturrichtlinie mehrstufig ausgestaltet: In § 2 Nr. 1 und Nr. 2 des deutschen SigG sind die Begriffe „elektronische Signatur" und „fortgeschrittene elektronische Signatur" in technologieneutraler Weise definiert. Dagegen ist die Definition der „qualifizierten elektronischen Signatur" in § 2 Nr. 3 des deutschen SigG technologiespezifisch (vgl. oben II.3.b) bb)): vorausgesetzt wird die Verwendung der asymmetrischen Kryptographie.

Das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr[43] stattet solche qualifizierten elektronischen Signaturen mit besonderer materiellrechtlicher Wirkung aus. Beispielsweise kann ein qualifiziert elektronisch

[27] *Ian A. Rambarran* (Fn. 8), S. 413 Fn. 64.
[28] *Anda Lincoln*, Electronic Signature Laws and the Need for Uniformity in the Global Market, in: The Journal of Small and Emerging Business Law 2004, S. 71.
[29] *Ian A. Rambarran* (Fn. 8), S. 413 Fn. 65, abrufbar unter http://www.ss.ca.gov/digsig/code165.htm (besucht am 19.05.2005).
[30] *Anda Lincoln* (Fn. 27), S. 73.
[31] *Ian A. Rambarran* (Fn. 8), S. 413 Fn. 58.
[32] *Anda Lincoln* (Fn 27), S. 73.
[33] *Jennifer L. Koger*, You, Sign, E-SIGN, We All Fall Down: Why the United States Should Not Crown the Marketplace as Primary Legislator of Electronic Signatures, in: Transnational Law and Contemporary Problems 2001, S. 507, 508.
[34] *Jennifer L. Koger* (Fn.32), S. 508-510.
[35] *Jennifer L. Koger* (Fn. 32), S. 510.
[36] *Jennifer L. Koger* (Fn. 32), S. 512.
[37] *Uwe Blaurock/Jürgen Adam* (Fn. 5), S. 95.
[38] *Uwe Blaurock/Jürgen Adam* (Fn. 5), S. 100.
[39] *Uwe Blaurock/Jürgen Adam* (Fn. 5), S. 114, in diesem Sinn auch *Jennifer L. Koger* (Fn. 32), S. 495.
[40] Gesetz über Rahmenbedingungen für elektronische Signaturen, Bundesgesetzblatt I 2001, S. 876 ff.
[41] Erstes Gesetz zur Änderung des Signaturgesetzes, Bundesgesetzblatt I 2005, S. 2 ff.; dazu *Alexander Roßnagel*, Elektronische Signaturen mit der Bankkarte? – Das Erste Gesetz zur Änderung des Signaturgesetzes, in: Neue Juristische Wochenschrift 2005, S. 385 ff.
[42] *Ulrich Noack* (Fn. 13), S. 1893.
[43] Bundesgesetzblatt I 2001, S. 1542 ff., in Kraft getreten am 01.08.2001.

signiertes elektronisches Dokument gem. § 126 a Abs. 1 BGB die gesetzlich vorgeschriebene Schriftform ersetzen.[44]

Am 1. April 2005 ist das Justizkommunikationsgesetz[45] in Kraft getreten. Es ermöglicht einen umfassenden elektronischen Rechtsverkehr mit den Gerichten und die Führung elektronischer Gerichtsakten. Das Justizkommunikationsgesetz sieht vor, dass elektronisch abgefasste Urteile mit einer qualifizierten elektronischen Signatur zu versehen sind, dies gilt grundsätzlich auch für elektronisch abgefasste bestimmende Schriftsätze. Weiter enthält das Gesetz Regelungen über die elektronische Akteneinsicht, über den Beweiswert elektronischer Dokumente und über den Medientransfer, also über die Umwandlung von Papierdokumenten in elektronische Dokumente.[46]

Die qualifizierte elektronische Signatur ist also sowohl materiellrechtlich als auch prozessrechtlich privilegiert, obgleich gem. § 1 Abs. 2 des deutschen SigG die Verwendung elektronischer Signaturen beliebiger Art[47] grundsätzlich freigestellt ist.

IV. Die Situation in der VR China vor dem 01.04.2005

Vor dem Inkrafttreten des Gesetzes der VR China über elektronische Signaturen gab es in China bereits in verschiedenen Bereichen Regelungen zu elektronischen Signaturen bzw. zum elektronischen Geschäftsverkehr.

1. Das Vertragsgesetz der VR China

Das „Vertragsgesetz der Volksrepublik China“[48] (VertragsG) bestimmt in § 11, dass der Schriftform (§ 10 Abs. 1 Alt. 1 VertragsG) genügt werden kann, indem elektronischer Datenaustausch, E-Mail oder andere Formen, die Inhalte sichtbar zum Ausdruck bringen können, verwendet werden. Die §§ 16 Abs. 2, 26 Abs. 2 und 34 Abs. 2 VertragsG enthalten für diesen Fall Regelungen zum Zugang von Antrag und Annahme sowie zum Ort des Vertragsschlusses. Jedoch kann in diesem Fall gem. § 33 Satz 1 VertragsG vor dem Zustandekommen des Vertrags die Unterzeichnung eines Bestätigungsschreibens verlangt werden; der Vertrag kommt dann erst mit Unterzeichnung dieses Bestätigungsschreibens zustande, § 33 Satz 2 VertragsG. Vorschriften zum Verfahren der elektronischen Signatur und deren Rechtswirkungen enthält das Vertragsgesetz nicht.

2. Zertifizierungsstellen

Trotz fehlender rechtlicher Anerkennung bestand Bedarf für den Einsatz elektronischer Signaturen. Um die Verwendung elektronischer Signaturen nach dem Public Key-Verfahren zu ermöglichen, wurden u. a. in Shanghai, Peking, Kanton, Shenzhen und Hainan die dafür benötigten Zertifizierungsstellen errichtet.[49] Im Finanzsektor hat ein Zusammenschluss von zwölf chinesischen Banken eigene Zertifizierungsstellen eingerichtet, um den Kunden Zertifizierungsdienste anbieten zu können.[50] Um die Tätigkeit dieser Zertifizierungsstellen zu regulieren, haben Hainan (09.08.2001), Shanghai (18.11.2002) und Kanton (06.12.2002) entsprechende Vorschriften erlassen.[51]

V. Das Gesetz der VR China über elektronische Signaturen

Das Gesetz der VR China über elektronische Signaturen umfasst 36 Paragraphen und ist in fünf Abschnitte gegliedert. Abschnitt 1 enthält allgemeine Vorschriften, Abschnitt 2 befasst sich mit elektronischen Dokumenten, Abschnitt 3 regelt elektronische Signatur und Zertifizierung, in Abschnitt 4 finden sich Haftungsvorschriften, und Abschnitt 5 enthält schließlich ergänzende Vorschriften.

1. Allgemeine Vorschriften

a) Gesetzeszweck

Zweck des Gesetzes ist es gem. § 1 SigG, die Verwendung elektronischer Signaturen zu regeln, elektronischen Signaturen rechtliche Wirksamkeit zu verleihen sowie die rechtmäßigen Rechte und Interessen aller Beteiligten zu schützen.

b) Begriffsbestimmungen

- „Elektronische Signaturen“ werden in § 2 Abs. 1 SigG definiert als in elektronischen Dokumenten in elektronischer Form enthaltene oder in elektronischer Form angefügte Daten, die dazu dienen, den

[44] Dies gilt allerdings (noch) nicht in den Fällen der §§ 484 I 2, 492 I 2, 623, 630, 761, 766, 780, 781 BGB.
[45] Bundesgesetzblatt I 2005, S. 837 ff.
[46] Newsletter des Bundesjustizministeriums vom 18.03.2005.
[47] Zu den Möglichkeiten der Verwendung fortgeschrittener elektronischer Signaturen: *Alexander Roßnagel*, Die fortgeschrittene elektronische Signatur, in: MultiMedia und Recht 2003, S. 164 ff.
[48] 中华人民共和国合同法 v. 15.03.1999, Amtsblatt des Staatsrates (国务院公报) 1999, Nr. 11, S. 388 ff.; deutsche Übersetzung und Einführung in: *Scheil/Gargulla/Schröder/Riemenschneider*, Vertragsgesetz der Volksrepublik China, Hamburg 1999.
[49] *GAO Fuping*, The E-Commerce Legal Environment in China: Status Quo and Issues, in: Temple International and Comparative Law Journal 2004, S. 56.
[50] *GAO Fuping* (Fn. 48), S. 57; *Ian A. Rambarran* (Fn. 8), S. 427.
[51] *GAO Fuping* (Fn. 48), S. 57.

Unterzeichner zu identifizieren und die Billigung des Inhalts durch den Unterzeichner erkennen zu lassen. Dies entspricht der oben (II.2.a)) dargestellten Definition.

- Gem. § 2 Abs. 2 SigG sind „elektronische Dokumente" Informationen, die auf elektronische, optische, magnetische oder ähnliche Weise erstellt, versendet, empfangen oder gespeichert werden. Dies entspricht der Regelung in Art. 2 lit. a MLES. Elektronische Dokumente sind also nicht nur mit Textverarbeitungsprogrammen erstellte Dateien, sondern beispielsweise auch E-Mails.

- „Unterzeichner" ist gem. § 34 Nr. 1 SigG, wer über die Signaturerstellungsdaten (legaldefiniert in § 34 Nr.5 SigG, vgl. unten) verfügt und für sich selbst oder im Namen einer durch ihn vertretenen Person eine elektronische Signatur verwendet. Diese Definition stimmt mit derjenigen des Art. 2 lit. d MLES überein.

- „Auf die elektronische Signatur vertrauender Beteiligter" ist gem. § 34 Nr. 2 SigG, wer aufgrund seines Vertrauens auf ein Signaturzertifikat (legaldefiniert in § 34 Nr. 3 SigG, vgl. unten) oder auf eine elektronische Signatur bestimmte Handlungen vornimmt. Diese Definition stimmt mit derjenigen des Art. 2 lit. f MLES überein.

- § 34 Nr. 3 SigG definiert in Übereinstimmung mit Art. 2 Nr. 9 RLeS und Art. 2 lit. B MLES „Signaturzertifikat" als elektronische Aufzeichnung, die die Verbindung zwischen dem Inhaber einer elektronischen Signatur und den Signaturerstellungsdaten beweisen kann.

- „Signaturerstellungsdaten" sind gem. § 34 Nr. 4 SigG Daten, die bei Verwendung einer elektronischen Signatur benutzt werden und die elektronische Signatur auf zuverlässige Weise dem Inhaber der elektronischen Signatur zuordnen. Dies ist bei Verwendung des Public Key-Verfahrens der private Signaturschlüssel.[52]

- Schließlich werden als „Signaturverifizierungsdaten" gem. § 34 Nr. 5 SigG diejenigen Daten, Kodes, Kennwörter, Algorithmen oder öffentliche Schlüssel bezeichnet, die zur Verifizierung der Signatur benutzt werden. Dies entspricht der Definition in Art. 2 Nr. 7 RLeS.

[52] So die ausdrückliche Regelung in Art. 2 Nr. 4 RLeS.

c) Verwendung elektronischer Signaturen und elektronischer Dokumente

§ 3 Abs. 1 SigG eröffnet die Möglichkeit, bei Urkunden auf dem Gebiet des bürgerlichen Rechts[53] elektronische Signaturen und elektronische Dokumente zu verwenden. Gem. § 3 Abs. 2 SigG darf solchen Urkunden die rechtliche Wirksamkeit nicht allein deshalb abgesprochen werden, weil elektronische Signaturen oder elektronische Dokumente verwendet wurden. Dies entspricht der Regelung in Art. 9 Abs. 1 S. 2 der Europäischen Richtlinie über den elektronischen Geschäftsverkehr (RLeG). [54] § 3 Abs. 3 SigG nimmt (wie auch Art. 9 Abs. 2 RLeG) bestimmte Bereiche von den Bestimmungen der Absätze 1 und 2 aus, wobei die Aufzählung nicht abschließend ist und Abs. 3 Nr. 3 anders als die RLeG ausdrücklich Urkunden ausnimmt, die die Einstellung von Leistungen öffentlicher Dienstleistungseinrichtungen betreffen.

2. Elektronische Dokumente

a) Erfüllung von Formerfordernissen durch elektronische Dokumente

Elektronische Dokumente gelten als der Schriftform entsprechend, wenn ihr Inhalt in körperlicher Form dargestellt werden kann und wenn sie jederzeit eingesehen und überprüft werden können, § 4 SigG. Wann die Schriftform gebraucht werden muss, bestimmt sich beispielsweise nach § 10 Abs. 2 Satz 1 VertragsG in Verbindung mit Spezialvorschriften. In § 5 SigG finden sich die Voraussetzungen, unter denen elektronische Dokumente als den Anforderungen der in Gesetzen und anderen Rechtsnormen vorgeschriebenen Form der Urschrift genügen: Ihr Inhalt muss effizient darstellbar sein und es muss die Möglichkeit jederzeitiger Einsichtnahme und Überprüfung bestehen; außerdem muss sichergestellt sein, dass ihr Inhalt seit der endgültigen Erstellung vollständig und unverändert geblieben ist. Die Vorlage der Urschrift ist z. B. in § 68 Abs. 1 Satz 1 des Zivilprozessgesetzes der VR China [55] für den Urkundenbeweis vorgeschrieben. Gem. § 6 SigG genügen elektronische Dokumente unter bestimmten Voraussetzungen den

[53] Zur Anwendbarkeit auf dem Gebiet des öffentlichen Rechts siehe unten V.5.

[54] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 08.06.2000 über bestimmte rechtliche Aspekte der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt.

[55] 中华人民共和国民事诉讼法, verabschiedet von der 4. Sitzung des 7. Nationalen Volkskongresses am 09.04.1991 (ZPG); deutsche Übersetzung von *Frank Münzel* unter http://lehrstuhl.jura.uni-goettingen.de/chinarecht/910409.htm (besucht am 10.05.2005).

Anforderungen der in Gesetzen und anderen Rechtsnormen vorgeschriebenen Aufbewahrung von Dokumenten. Die Aufbewahrung von Dokumenten wird beispielsweise in § 99 der „Regelungen des Obersten Volksgerichts zu einigen Fragen der Verhandlung von Konkursfällen“ [56] verlangt.

b) Verwendung von elektronischen Dokumenten als Beweismittel

Zur Verwendung von elektronischen Dokumenten als Beweismittel bestimmt § 7 SigG, dass diese nicht allein deshalb, weil es sich um elektronische Dokumente handelt, nicht zugelassen werden dürfen. Zur gem. § 63 II ZPG vorzunehmenden Beweiswürdigung gibt § 8 SigG dem Gericht einige Kritierien für die Überprüfung der Echtheit elektronischer Dokumente an die Hand.

c) Abgabe und Zugang von in elektronischen Dokumenten enthaltenen Willenserklärungen

Die Regelung bezüglich des Zugangs von elektronischen Dokumenten in den §§ 16 Abs. 2, 26 Abs. 2 VertragsG wird in § 11 Abs. 2 SigG unverändert wiederholt. § 10 Satz 2 SigG bestimmt, dass ein elektronisches Dokument in dem Zeitpunkt als zugegangen gilt, in dem der Absender eine Empfangsbestätigung erhalten hat. Bezüglich der Abgabe bestimmt § 11 Abs. 1 SigG, dass ein elektronisches Dokument in dem Zeitpunkt als versendet gilt, in dem es in ein anderes als das vom Versender kontrollierte Nachrichtensystem eintritt. Hinsichtlich des Ortes der Versendung und des Empfangs wiederholt § 12 SigG die in § 34 Abs. 2 VertragsG enthaltene Regelung. Die Festlegung der Hauptgeschäftsniederlassung und ersatzweise des gewöhnlichen Aufenthaltsortes als Ort der Versendung bzw. des Empfangs ist notwendig, da der tatsächliche Ort, an dem ein elektronisches Dokument in ein Nachrichtensystem eintritt, in der Regel der Standort des jeweiligen Nachrichtenservers ist. Dieser ist den Parteien aber in der Regel unbekannt, ändert sich möglicherweise im Verlauf einer langwierigen Korrespondenz und kann überdies in einem fremden Staat liegen, dessen Recht dann eigentlich angewendet werden müsste. Die §§ 9 und 10 Satz 1 SigG schließlich betreffen Fragen der Bestimmung des Absenders bzw. der Verwendung von Empfangsbestätigungen.

3. Elektronische Signatur und Zertifizierung

a) Elektronische Signatur

In § 13 Abs. 1 SigG werden die Voraussetzungen genannt, die eine zuverlässige elektronische Signatur erfüllen muss: Die Signaturerstellungsdaten müssen zur Zeit der Verwendung zur Erzeugung einer elektronischen Signatur ausschließlich dem Inhaber der elektronischen Signatur zugeordnet sein, sie müssen außerdem bei der Unterzeichnung ausschließlich unter der Kontrolle des Inhabers der elektronischen Signatur stehen, weiter muss jede Veränderung der elektronischen Signatur, des Inhalts oder der Form des elektronischen Dokuments nach der Unterzeichnung erkennbar sein. Diese Regelung stellt keinen Bezug zu einem bestimmten Verfahren der Erzeugung elektronischer Signaturen her, sie ist also technologieneutral, und entspricht inhaltlich der Definition der „fortgeschrittenen elektronischen Signatur“ in Art. 2 Nr. 2 RLeS und den in Art. 6 Abs. 3 MLES vorgeschlagenen Voraussetzungen. § 14 SigG verleiht zuverlässigen elektronischen Signaturen die gleiche rechtliche Wirksamkeit wie eigenhändigen Unterschriften oder Siegeln. Das Problem, dass gem. § 33 VertragsG bei Vertragsschluss per E-Mail die Unterzeichnung eines Bestätigungsschreibens verlangt werden kann, wodurch ein vollständig elektronisch abgewickelter Vertragsschluss vereitelt werden konnte, ist damit gelöst. Gem. § 13 Abs. 2 SigG steht es den Beteiligten jedoch frei, andere elektronische Signaturen als die zuverlässige elektronische Signatur nach § 13 Abs. 1 SigG zu verwenden und Voraussetzungen für deren Zuverlässigkeit vereinbaren. Auch hier zeigt sich wieder die Technologieneutralität des § 13 SigG. Ein ähnlicher Regelungsvorschlag findet sich in Art. 6 Abs. 4 lit. a MLES. In § 15 SigG werden dem Unterzeichner Sorgfaltspflichten auferlegt, deren Verletzung gem. § 27 SigG sanktioniert wird (vgl. dazu unten V.4.).

b) Zertifizierung

Obwohl das Gesetz technologieneutral ausgestaltet ist, enthält es Vorschriften über Zertifizierungsdienste. Zwar werden diese nur bei Verwendung des Public Key-Verfahrens benötigt, jedoch stellen die betreffenden Vorschriften keine Ausnahme zur sonstigen Technologieneutralität dar; vielmehr ermöglicht gerade die Festlegung von Standards für das Anbieten von Zertifizierungsdiensten, dass das Public Key-Verfahren eine verlässliche unter mehreren Varianten der

[56] 最高人民法院《关于审理企业破产案件若干问题的规定》法释 [2002] 23 号, Amtsblatt des Obersten Volksgerichts 2002/5, 155 ff.

elektronischen Signatur darstellt. Außerdem existierten bereits vor dem Inkrafttreten des Gesetzes Zertifizierungsdiensteanbieter (vgl. oben IV.2.), so dass es angebracht erschien, deren Tätigkeit einheitlich zu regeln. Nach § 25 SigG ist die für die Informationsindustrie zuständige Abteilung des Staatsrats dafür zuständig, konkrete Verwaltungsmaßnahmen festzulegen und die Zertifizierungsdiensteanbieter zu beaufsichtigen. Die für die Informationsindustrie zuständige Abteilung des Staatsrats ist das Ministerium für die Informationsindustrie; es hat von dieser Rechtssetzungsermächtigung bereits Gebrauch gemacht und eine Zertifizierungsdiensteverwaltungsmaßnahme[57] (ZDVM) festgelegt.

aa) Zertifizierungsdiensteanbieter

Gem. § 16 SigG erbringen bei Bedarf, also wenn Signaturen nach dem Public Key-Verfahren erstellt werden sollen, Zertifizierungsdiensteanbieter die erforderlichen Zertifizierungsdienstleistungen. § 17 SigG nennt die Anforderungen, die Zertifizierungsdiensteanbieter hinsichtlich ihrer personellen, technischen, finanziellen und organisatorischen Ausstattung erfüllen müssen. Konkretisiert wird dies durch § 5 ZDVM, danach müssen die Diensteanbieter im Einzelnen: (1) die Eigenschaft einer unabhängigen juristischen Person haben; (2) über eine Belegschaft von mindestens 30 Personen, bestehend aus technischem Fachpersonal, Unternehmensleitung, Sicherheitspersonal und Kundenbetreuungspersonal, verfügen; (3) über mindestens RMB 30 Mio. Yuan registriertes Kapital verfügen; (4) über eine ständige Betriebsstätte und ein den Anforderungen des Anbietens von Zertifizierungsdiensten genügendes physikalisches Umfeld verfügen; (5) über den staatlichen Sicherheitsstandards entsprechende Technologie und Ausstattung verfügen; (6) über eine Bescheinigung verfügen, dass das staatliche Kryptographieverwaltungsorgan die Verwendung von Kryptographie genehmigt hat; (7) andere durch Gesetz oder Verwaltungsrechtsnorm bestimmte Voraussetzungen erfüllen. Gem. § 33 ZDVM dürfen während der Gültigkeitsdauer der Zertifizierungslizenz (dazu sogleich bb)) die bei Errichtung vorliegenden Voraussetzungen nicht unterschritten werden.

bb) Genehmigung von Zertifizierungsdiensten

In § 18 SigG wird ein Genehmigungsvorbehalt statuiert und das Genehmigungsverfahren beschrieben. Einige Details werden erst durch die §§ 6 bis 14 ZDVM geregelt. § 6 ZDVM bestimmt, dass der Antrag auf Genehmigung schriftlich und unter Vorlage von Nachweisen über das beschäftigte technische Fach- und Verwaltungspersonal und über das Kapital und die Betriebsstätte zu stellen ist. Bevor das Ministerium für die Informationsindustrie die materielle Prüfung des Antrags vornimmt (§ 8 ZDVM), entscheidet es zunächst über dessen Zulässigkeit (§ 7 ZDVM). Ist der Antrag zulässig, so muss das Ministerium für die Informationsindustrie im Rahmen der materiellen Prüfung Stellungnahmen des Handelsministeriums und anderer zuständiger Abteilungen einholen (§ 18 Abs. 1 Satz 2 SigG i.V.m. § 9 ZDVM). Die beiden letztgenannten Aspekte machen das Verfahren unübersichtlich und dessen Ergebnis schwer abschätzbar. Eine für die Praxis interessante Vorschrift, die offenbar die Objektivität des Genehmigungsverfahrens wahren soll, enthält § 8 Satz 2 ZDVM: Wenn bei Prüfung der Antragsunterlagen durch das Ministerium für Informationsindustrie eine Überprüfung der Richtigkeit der enthaltenen Angaben erforderlich ist, so werden zur Untersuchung vor Ort mindestens zwei Mitarbeiter entsandt.

Wenn die Genehmigung erteilt wird (§ 18 Abs. 1 Satz 3 Halbsatz 1 SigG), muss das Ministerium für die Informationsindustrie gem. § 10 Abs. 1 Satz 2 Halbsatz 2 ZDVM folgende Punkte bekannt machen: (1) die Nummer der Zertifizierungslizenz; (2) die Bezeichnung des Zertifizierungsdiensteanbieters; (3) das ausstellende Organ und das Ausstellungsdatum. Gem. § 10 Abs. 2 ZDVM sind Veränderungen bekanntzumachen. Die Zertifizierungslizenz gilt für fünf Jahre (§ 10 Abs. 3 ZDVM) und kann gem. § 14 ZDVM auf Antrag verlängert werden. Die Vorschrift des § 18 Abs. 3 SigG wird durch § 12 ZDVM konkretisiert; der Zertifizierungsdiensteanbieter muss nach Erhalt der Zertifizierungslizenz vor Aufnahme seiner Tätigkeit im Internet bekanntmachen: (1) seine Bezeichnung und seinen gesetzlichen Vertreter; (2) seine Adresse und eine Möglichkeit der Kontaktaufnahme; (3) die Nummer der Zertifizierungslizenz; (4) ausstellendes Organ und Ausstellungsdatum; (5) Beginn und Ende der Gültigkeit der Zertifizierungslizenz. Ändert sich innerhalb der Gültigkeitsdauer der Zertifizierungslizenz die Firma, die Adresse, das registrierte Kapital

[57] 电子认证服务管理办法, Dekret des Ministeriums für die Informationsindustrie Nr. 35 vom 08.02.2005, in Kraft getreten am 01.04.2005, abrufbar unter http://www.chinacourt.org/flwk/show1.hp?file_id =99822&PHPSESSID=955cb6b985bf3b61c5c80c8efb41db03 (besucht am 19.05.2005).

oder der gesetzliche Vertreter, so muss der Zertifizierungsdiensteanbieter dies innerhalb von fünf Tagen nach Abschluss der betreffenden Formalitäten im Internet bekanntmachen sowie innerhalb von 15 Tagen nach der Bekanntmachung beim Ministerium für die Informationsindustrie aktenkundig machen, § 13 ZDVM.

Zertifizierungsdiensteanbieter, die ihre Tätigkeit bereits vor dem Inkrafttreten des SigG aufgenommen haben (vgl. oben IV.2), bedürfen ebenfalls einer Zertifizierungslizenz, wenn sie ihre Dienste auch nach dem 30.09.2005 noch anbieten wollen; die Lizenz ist bis spätestens 30.09.2005 einzuholen, § 41 ZDVM.

cc) Zertifizierungsregeln

Nach § 19 SigG müssen die Zertifizierungsdiensteanbieter Zertifizierungsregeln festlegen, die den einschlägigen staatlichen Bestimmungen [58] entsprechen. Gem. § 15 Abs. 1 ZDVM müssen die Zertifizierungsregeln durch den Zertifizierungsdiensteanbieter vor Aufnahme seiner Tätigkeit bekanntgemacht und beim Ministerium für die Informationsindustrie aktenkundig gemacht werden. Änderungen der Zertifizierungsregeln müssen ebenfalls bekanntgemacht und binnen 30 Tagen nach der Bekanntmachung beim Ministerium für die Informationsindustrie aktenkundig gemacht werden. § 16 ZDVM bestimmt, dass die Zertifizierungsdiensteanbieter ihre Dienste entsprechend den von ihnen bekanntgemachten Zertifizierungsregeln anbieten müssen.

dd) Signaturzertifikate

Die Beantragung und Erteilung von Signaturzertifikaten sowie der Inhalt der Signaturzertifikate sind in den §§ 20 und 21 SigG geregelt. Unter anderem müssen Signaturzertifikate gem. § 21 Nr. 5, Nr. 6 SigG die Signaturverifizierungsdaten des Inhabers des Zertifikats sowie die elektronische Signatur des Zertifizierungsdiensteanbieters enthalten. Die in § 21 SigG formulierten Anforderungen sind auch in § 28 ZDVM zu finden. Die im Gesetz nicht angesprochene Möglichkeit des Widerrufs von Signaturzertifikaten ist in § 29 ZDVM normiert. Der Zertifizierungsdiensteanbieter kann ein Signaturzertifikat z. B. dann widerrufen, wenn der Inhaber dies beantragt, wenn der Inhaber falsche Angaben gemacht hat oder seinen vertraglichen Pflichten gegenüber dem Zertifizierungsdiensteanbieter nicht nachkommt oder wenn die Sicherheit des Signaturzertifikats nicht garantiert werden kann.

ee) Pflichten der Zertifizierungsdiensteanbieter

Die Garantiepflichten des Zertifizierungsdiensteanbieters sind in § 22 SigG und in § 18 Abs. 1 und 2 ZDVM geregelt. Die Pflicht zur Datenspeicherung ergibt sich aus § 24 SigG und aus § 18 Abs. 3 ZDVM; § 20 ZDVM verpflichtet zusätzlich zur Geheimhaltung der Daten des Inhabers der elektronischen Signatur und der Daten auf die Signatur vertrauender Beteiligter. § 21 ZDVM legt fest, dass der Zertifizierungsdiensteanbieter den Antragsteller über folgende Punkte informieren muss: (1) die Voraussetzungen der Verwendung von Signaturzertifikaten und elektronischen Signaturen; (2) gebührenpflichtige Dienstleistungen und Höhe der Gebühren; (3) die Befugnis und Verpflichtung zur Speicherung und Verwendung der Daten des Zertifikatsinhabers; (4) den Umfang der Haftung des Zertifizierungsdiensteanbieters; (5) den Umfang der Haftung des Zertifikatsinhabers; (7) andere Punkte, über die im voraus informiert werden muss.

Die in § 23 SigG für den Fall der vorläufigen oder endgültigen Einstellung der Tätigkeit festgeschriebenen Pflichten zur Benachrichtigung der Beteiligten und der Behörden sowie zur Regelung der Übernahme der Tätigkeit durch einen anderen Zertifizierungsdiensteanbieter sind auch in den §§ 23 bis 27 ZDVM zu finden bzw. werden dort konkretisiert. Die §§ 34, 35 ZDVM verpflichten die Zertifizierungsdiensteanbieter, das Ministerium für die Informationsindustrie zu statistischen Zwecken über die Entwicklung ihrer Zertifizierungstätigkeit zu unterrichten bzw. Maßnahmen zur Qualifizierung ihrer Mitarbeiter durchzuführen.

ff) Aufsicht

Die in § 25 SigG vorgesehene Aufsicht über die Zertifizierungsdiensteanbieter wird in § 32 ZDVM dahingehend näher erläutert, dass das Ministerium für die Informationsindustrie jährliche Untersuchungen durchführt und deren Ergebnis veröffentlicht, wobei die Untersuchungen aus der Prüfung von Berichten und aus Kontrollen vor Ort bestehen. Gem. § 36 ZDVM können bei Bedarf konkrete Aufsichtsaufgaben den für die Informationsindustrie zuständigen Abteilungen der

[58] Es handelt sich dabei um den gemäß § 15 Abs. 1 der Maßnahmen vom Ministerium für Informationsindustrie bekannt gemachten „Standard für die Regeln der Zertifizierungsgeschäfte" (电子认证业务规则规) siehe im Internet unter http://211.152.106.51/declare/yuwubiaozhun.html, der zur „vorläufigen Durchführung" (试行) vom Büro zur Verwaltung der Zertifizierungsdienstleitungen des Ministeriums für Informationsindustrie im April 2005 erlassen wurde.

betreffenden Provinzen, autonomen Gebiete oder regierungsunmittelbaren Städte übertragen werden.

gg) Ausländische Zertifikate

In § 26 SigG ist bestimmt, dass ausländische Signaturzertifikate im Inland anzuerkennen sind, wenn die für die Informationsindustrie zuständige Abteilung des Staatsrats sie gemäß einschlägiger Abkommen oder gemäß dem Gegenseitigkeitsprinzip zugelassen hat. Eine entsprechende Regelung trifft auch § 42 ZDVM. Das Pendant dieser Vorschrift im deutschen Signaturgesetz ist § 23 Abs. 1 S. 2 des deutschen SigG.

4. Haftung

Die §§ 27 und 28 SigG statuieren die Voraussetzungen der Schadensersatzhaftung des Inhabers einer elektronischen Signatur bzw. des Zertifizierungsdiensteanbieters, wobei § 28 SigG eine Beweislastumkehr zu Lasten des Zertifizierungsdiensteanbieters vorsieht. § 29 SigG regelt Verwaltungssanktionen für den Fall des Anbietens von Zertifizierungsdiensten ohne Genehmigung, § 30 SigG für den Fall der Verletzung der Meldepflicht aus § 23 Abs. 2 SigG und § 31 SigG für sonstige Pflichtverletzungen. Weitere Sanktionen sind in den ZDVM vorgesehen: Verheimlicht ein Zertifizierungsdiensteanbieter gegenüber dem Ministerium für die Informationsindustrie Umstände von Bedeutung, macht er falsche Angaben oder verweigert er Angaben über seine Aktivitäten, so ordnet das Ministerium gem. § 37 ZDVM im Rahmen seiner Befugnisse Abhilfe an und spricht eine Abmahnung aus oder verhängt eine Geldbuße in Höhe von RMB 5.000 bis 10.000 Yuan. Bietet der Zertifizierungsdiensteanbieter seine Dienste entgegen § 16 ZDVM nicht entsprechend seinen Zertifizierungsregeln an oder erfüllt er seine Pflicht aus § 27 ZDVM zur Übernahme der Geschäftstätigkeit eines anderen Zertifizierungsdiensteanbieters auf Anordnung des Ministeriums für die Informationsindustrie nicht, so ordnet dieses im Rahmen seiner Befugnisse Abhilfe innerhalb einer bestimmten Frist an und spricht eine Abmahnung aus und/oder verhängt eine Geldbuße von höchstens RMB 10.000 Yuan, § 39 ZDVM. Verletzt der Zertifizierungsdiensteanbieter seine Pflicht aus § 33 ZDVM, während der Gültigkeitsdauer der Zertifizierungslizenz die bei Errichtung vorliegenden Voraussetzungen nicht zu unterschreiten, ordnet gem. § 40 ZDVM das Ministerium für die Informationsindustrie im Rahmen seiner Befugnisse Abhilfe innerhalb einer bestimmten Frist an und verhängt eine Geldbuße von höchstens RMB 30.000 Yuan.

In § 32 SigG wird klargestellt, dass das Fälschen, die betrügerische Verwendung oder das Entwenden der elektronischen Signatur eines anderen strafrechtliche Verfolgung und zivilrechtliche Haftung nach sich ziehen kann. Die in § 33 SigG vorgesehene Disziplinarstrafe im Fall der Amtspflichtverletzung besteht gem. § 38 ZDVM je nach Schwere der Umstände in einer Abmahnung, einem Aktenvermerk als Vergehen, einem Aktenvermerk als schweres Vergehen, einer Degradierung, der Amtsenthebung oder der Entfernung aus dem Amt.

5. Ergänzende Vorschriften

In § 35 SigG ist die Möglichkeit vorgesehen, dass der Staatsrat oder vom Staatsrat bestimmte Abteilungen das konkrete Verfahren der Verwendung elektronischer Signaturen und elektronischer Dokumente bei staatlichen und gesellschaftlichen Aktivitäten festlegen. Dies ist bisher noch nicht geschehen. Möglicherweise möchte man zunächst Erfahrungen mit dem Einsatz der neuen Technologien im Bereich des Zivilrechts sammeln, bevor man sie auch für den sensibleren Bereich der öffentlichen Verwaltung zulässt. Denkbar ist der Einsatz elektronischer Signaturen und Dokumente in der Kommunikation innerhalb der oder zwischen den Behörden und darüber hinaus in der Kommunikation zwischen Behörden und Bürgern. Es wird darauf hingewiesen, dass ein Nebeneinander des Behördenverkehrs in herkömmlicher Papierform einerseits und auf elektronischem Wege andererseits die Kosten der Verwaltung erhöhen könnte.[59] Dies mag kurzfristig zwar zutreffen; mittel- bis langfristig könnte der Einsatz elektronischer Medien in der Verwaltung die Kosten aber wohl senken – eine hinreichende Akzeptanz und entsprechende Nutzung des Angebots durch die Bürger vorausgesetzt. Außerdem wird die Frage aufgeworfen, ob es sinnvoll wäre, den Behörden von privaten Zertifizierungsdiensteanbietern Signaturzertifikate ausstellen zu lassen oder ob nicht vielmehr die Zentralregierung diese Aufgabe übernehmen sollte.[60]

VI. Fazit und Ausblick

Mit der Gleichstellung von elektronischen Dokumenten und Papierdokumenten (§ 4 SigG), der

[59] *LI Guangqian* (李广乾) im Interview mit *FAN Sili* (范思立), Chinesische Wirtschaftszeitschrift (中国经济时报), 05.04.2005, http://www.law-lib.com/fzdt/newshtml/szpl/20050405103054.htm (besucht am 10.05.2005).

[60] *LI Guangqian* (李广乾) im Interview mit *FAN Sili* (范思立) (Fn. 57).

Gleichstellung zuverlässiger elektronischer Signaturen mit eigenhändigen Unterschriften oder Siegeln (§ 14 SigG) und elektronischer Dokumente mit Urschriften (unter den Voraussetzungen des § 5 SigG) schafft das Gesetz der VR China über elektronische Signaturen wichtige Voraussetzungen für den elektronischen Geschäftsverkehr. Der technologieneutrale Ansatz des Gesetzes lässt Spielraum für künftige Entwicklungen. Die Vereinheitlichung der Vorschriften über Zertifizierungsdienste und die behördliche Kontrolle der Zertifizierungsdiensteanbieter wird das Vertrauen in elektronische Signaturen nach dem Public Key-Verfahren und damit die bereits bestehende Tendenz zugunsten der asymmetrischen Kryptographie noch verstärken.

Nun bleibt abzuwarten, in welchem Maß sich die neuen rechtlichen Voraussetzungen auf die Praxis auswirken. In Deutschland ist der Einsatz elektronischer Signaturen und elektronischer Dokumente bis heute nicht sehr weit verbreitet,[61] obwohl zunächst durchaus optimistische Stimmen zu vernehmen waren.[62] Die Verbreitung elektronischer Signaturverfahren ist in erster Linie eine Frage der Infrastruktur.[63] Unter diesem Gesichtspunkt kann in China allenfalls in Ballungszentren und in den gut entwickelten Küstenregionen mit einer Nutzung der neuen Möglichkeiten auf breiter Basis gerechnet werden.

[61] *Alexander Roßnagel* (Fn. 40), S. 385.
[62] *Wendelin Bieser* (Fn. 14), S. 34.
[63] *Alexander Roßnagel* (Fn. 40).