

**Die elektronische Signatur  
Gutachten**

**März 2006**

**Georg Berger  
Lena Weißinger**

## Gutachten – Die elektronische Signatur

Dieses Gutachten behandelt die Funktionsweise und Anwendung qualifizierter elektronischer Signaturen unter Berücksichtigung der aktuellen Gesetzeslage. Da über [www.rechnung.de](http://www.rechnung.de) der Versand von Rechnungen ausschließlich per Email mit qualifizierter elektronischer Signatur angeboten wird, werden vorliegend die elektronische Übermittlung von Rechnungen durch EDI-Verfahren oder per Telefax nicht im Detail behandelt.

### 1. Funktionsweise der elektronischen Signatur

Eine elektronische Signatur ist – vereinfacht ausgedrückt – ein digitales Siegel, welches bei der digitalen Übermittlung von Daten den Absender zweifelsfrei identifiziert (Authentizität) und den Originalzustand der transportierten Daten gewährleistet (Integrität).

Die Funktionsweise der elektronischen Signatur basiert auf einem mathematisch-kryptografischen Verfahren, in dem als Grundlage für jede Person ein einmaliges Schlüsselpaar geschaffen wird:

- ein **privater Schlüssel** (Private Key) und
- ein **öffentlicher Schlüssel** (Public Key).

Diese beiden Schlüssel stehen in einer speziellen mathematischen Abhängigkeit zueinander, können aber nicht voneinander abgeleitet werden. Da der Signiervorgang an den privaten Schlüssel gebunden ist, handelt es sich hierbei stets um einen geheimen Schlüssel, der ausschließlich dem Absender bekannt ist. Im Gegensatz hierzu ist der öffentliche Schlüssel möglichst weit zu verbreiten. Auf diese Weise kann der Empfänger das durch den privaten Schlüssel erzeugte Siegel mit dem korrespondierenden öffentlichen Schlüssel öffnen und die Authentizität des Absenders sowie die Integrität der Daten zweifelsfrei verifizieren.

Die einmaligen Schlüsselpaare werden durch anerkannte Stellen natürlichen Personen fest zugeordnet. Diese Zuordnung durch akkreditierte Trust Center (ZDA - Zertifizierungdiensteanbieter) wird durch ein Signaturschlüssel-Zertifikat beglaubigt, welches der Signaturschlüssel-Inhaber erhält, so dass er es signierten Daten für deren Überprüfung beifügen kann. Mit Hilfe des dazugehörigen öffentlichen Schlüssels kann die

Signatur jederzeit überprüft und damit der Signaturschlüssel-Inhaber und die Unverfälschtheit der Daten festgestellt werden.

## **2. Verschlüsselung**

Die elektronische Signatur ist nicht zu verwechseln mit einer Verschlüsselung des signierten Dokuments selbst. Der Inhalt der signierten Datei bleibt unabhängig von dem gewählten Sicherheitsstandard für jeden lesbar.

Beim Empfänger einer qualifizierten elektronische Signatur wird mit Hilfe des öffentlichen Schlüssels des Senders und eines mathematischen Verfahrens (Hash-Code) lediglich überprüft, ob die erhaltene Signatur mit dem zugehörigen Signaturschlüssel erstellt worden ist und das Dokument nicht verändert wurde.

## **3. Sicherheit**

Das System der elektronischen Signatur basiert auf einem komplizierten mathematischen Verfahren, welches auf Primzahlen beruht. Die Sicherheit resultiert vor allem daraus, dass die Berechnung des einen Schlüssels aus dem anderen sehr aufwendig ist.

Selbst ein Verbund aus vielen Rechnern mit der heute verfügbaren Rechenleistung würde mehrere Jahre arbeiten, um einen einzigen Schlüssel zu errechnen. Eine hundertprozentige Sicherheit gibt es aber auch hier nicht.

## **4. Die gesetzlichen Rahmenbedingungen**

Im Signaturgesetz (SigG) und in der Verordnung zum Signaturgesetz (SigV) werden die elektronischen Signaturen selbst und insbesondere die Anforderungen an elektronische Signaturen und Zertifizierungsanbieter (ZDA) definiert. Die Rahmenbedingungen, wann welche elektronische Signatur verwendet werden kann oder muss beruhen im Wesentlichen auf dem Bürgerlichen Gesetzbuch (BGB) und anderen Gesetzen sowie Rechts- und Verwaltungsverordnungen.

Nach § 2 Nr. 1 SigG handelt es sich bei einer elektronischen Signatur *„um Daten in elektronischer Form, die anderen elektronischen Daten beigelegt oder logisch mit ihnen verknüpft ist und die zur Authentifizierung dient.* Eine solche elektronische Signatur hat per se keinen Sicherheitswert, da auch eine ohne weiteres kopierbare oder entfernbare

eingescannte Unterschrift diese Voraussetzungen erfüllt. Sie gewährleistet in keiner Weise die Integrität des Dokuments oder die Authentizität seines Ausstellers.

Rechtliche Relevanz hingegen haben drei besondere Arten der elektronischen Signatur, die sich nach ihren verschiedenen hohen Sicherheits-, Nachweis- und Kontrollniveaus unterscheiden:

- die fortgeschrittene elektronische Signatur, 2 Nr. 2 SigG,
- die qualifizierte elektronische Signatur, § 2 Nr. 3 SigG und
- die qualifizierte elektronische Signatur mit Akkreditierung, § 15 SigG.

#### **a. Die fortgeschrittene elektronische Signatur**

Die Regelung des § 2 Nr. 2 SigG fordert für die fortgeschrittene elektronische Signatur die Gewährleistung, die Signatur dem Schlüsselhaber zuzuordnen, die Möglichkeit, diesen zu identifizieren, und die Möglichkeit, die Signaturschlüssel unter dessen alleiniger Kontrolle zu halten, ohne dabei spezifische Qualitätsanforderungen zu stellen.

Mit der fortgeschrittenen elektronischen Signatur wird ein mittleres Sicherheitsniveau zwischen der einfachen und der qualifizierten Signatur bezweckt, aufgrund dessen aber viele Manipulationsmöglichkeiten bleiben. Aufgrund der mangelnden Sicherheit fortgeschrittener Signaturverfahren wurden diese vom europäischen und vom deutschen Gesetzgeber daher auch als ungeeignet angesehen, die eigenhändige Unterschrift zu ersetzen. Die Manipulationsmöglichkeit im Einzelfall wirkt sich auf die Beweiseignung der nach diesem Verfahren erzeugten Signaturen aus (siehe unten).

#### **b. Die qualifizierte elektronische Signatur**

Gemäß § 2 Nr. 3 SigG zeichnet sich eine qualifizierte elektronische Signatur – zusätzlich zu den Voraussetzungen einer fortgeschrittenen elektronischen Signatur – dadurch aus, dass sie auf einem qualifizierten Zertifikat beruht und mit einer sicheren Signaturerstellungseinheit erzeugt wird.

Ein qualifiziertes Zertifikat enthält die in § 7 SigG niedergelegten Angaben wie etwa Namen (oder Pseudonym), Signaturschlüssel und Gültigkeitszeitraum. Weiter muss gewährleistet sein, dass der Zertifizierungsdiensteanbieter Personen, die ein qualifiziertes Zertifikat beantragen, zuverlässig identifiziert. Eine sichere Signaturerstellungseinheit ist insbesondere der Chip der Signaturkarte, der den übergebenen Hashwert (Prüfsumme der zu signierenden Daten) verschlüsselt und die elektronische Signatur erstellt.

### **c. Die qualifizierte elektronische Signatur mit Akkreditierung**

Bei der qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung handelt es sich um eine Sonderform der qualifizierten elektronischen Signatur und gleichzeitig die höchste und in der Umsetzung anspruchsvollste Sicherheitsstufe.

Hierfür müssen qualifizierte elektronische Signaturen zum Zeitpunkt ihrer Erzeugung auf einem gültigen qualifizierten Zertifikat eines akkreditierten Zertifizierungsdiensteanbieters (ZDA) beruhen.

Mit der Anbieter-Akkreditierung verlangt der Gesetzgeber, dass der ZDA ein freiwilliges Akkreditierungsverfahren nach § 15 SigG durchlaufen hat. Dabei wird ein Gütezeichen erteilt, das belegt, dass die erforderlichen gesetzlichen Vorschriften erfüllt werden; insbesondere wird das Sicherheitskonzept umfassend auf seine Eignung und praktische Umsetzung geprüft, § 15 Abs.2 SigG.

## **5. Wahrung gesetzlicher und vereinbarter Schriftform**

### **a. Die gesetzliche Schriftform**

Zur Wahrung der gesetzlichen Schriftform bedarf es der qualifizierten elektronischen Signatur oder der qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung.

In verschiedenen Gesetzen und Rechtsverordnungen wird für manche Willenserklärungen die Schriftform nach § 126 BGB gefordert. Soll diese Schriftform durch eine elektronische Form ersetzt werden, bedarf es gemäß § 126 a BGB einer qualifizierten elektronischen Signatur oder einer qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung.

Für Verträge gilt der dem § 126 Abs. 2 BGB nachgebildete § 126a Abs. 2 BGB. Zur Wahrung der Form genügt nicht, dass jede Partei nur ihre eigene Angebots- und Annahmeerklärung signiert. Es müssen vielmehr gleichlautende Dokumente hergestellt werden, die den gesamten Vertragstext enthalten.

Zusätzlich wird in verschiedenen Gesetzen ohne Verweis auf die gesetzliche Schriftform bereits explizit eine qualifizierte elektronische Signatur (manchmal mit Anbieterakkreditierung oder langfristiger Überprüfbarkeit) zur Unterzeichnung von elektronischen Dokumenten vorgeschrieben.

### **b. Die vereinbarte Schriftform**

Ohne gesetzliche Notwendigkeit wird für Geschäftsvereinbarungen und Willenserklärungen zur besseren Beweisfähigkeit der getroffenen Vereinbarungen in einem eventuellen Rechtsstreit freiwillig Schriftform vereinbart. Auch auf diese vereinbarte Form ist die Regelung des § 126 a BGB entsprechend anzuwenden, § 127 Abs. 1 BGB. Hingegen bestimmt § 127 Abs. 2 BGB, dass zur Wahrung der Form genügt, dass – soweit nicht ein anderer Wille anzunehmen ist – die telekommunikative Übermittlung und bei einem Vertrag der Briefwechsel genügt.

Für elektronische Vereinbarungen, die freiwillig erstellt werden und auch elektronisch signiert werden sollen, müssen gemäß §127 Abs. 3 BGB keine qualifizierten elektronischen Signaturen verwendet werden.

Allerdings sollte das vereinbarte Signaturverfahren in der elektronisch signierten Vereinbarung genannt werden, da „im Zweifel“ die Unterzeichner von der Verwendung einer qualifizierten elektronischen Signatur ausgehen können und gegebenenfalls die Nachsignierung mittels einer qualifizierten elektronischen Signatur verlangen können.

## **6. Beweiseignung und Beweiskraft der elektronischen Signatur**

### **a. Beweis durch Augenschein**

Ein mit einer elektronischen Signatur versehenes elektronisches Dokument kann in einem Streitverfahren als Objekt des Augenscheins nach § 371 ZPO als Beweismittel eingeführt werden. Dies gilt auch für einfache und fortgeschrittene elektronische Signaturen.
--

Aufgrund der bereits dargestellten Manipulationsmöglichkeiten und Sicherheitsschwachstellen kann der Beweiswert einer einfachen oder fortgeschrittenen elektronischen Signatur aber nur gering sein.

#### **b. Beweiskraft elektronischer Dokumente**

Bürgerliches Recht und Zivilprozessrecht setzen als Medium im Rechtsverkehr und im Prozess regelmäßig eine in Papier verkörperte Urkunde voraus. Zwar ist die Urkunde zivilrechtlich nicht im Gesetz definiert, man versteht hierunter jedoch ein Beweismittel, dass die beweiserhebliche Gedankenerklärung dauerhaft verkörpert und den Aussteller erkennen lässt.

Auf elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, sind nach § 371a ZPO die Vorschriften über die Beweiskraft privater Urkunden entsprechend anwendbar, d.h. solche Dokumente werden wie (Papier-) Urkunden behandelt.

§ 371a Abs. 2 sieht eine Beweiserleichterung des Empfängers einer in elektronischen Form abgegebenen Erklärung vor. Ergibt eine Überprüfung nach dem SigG den Anschein, dass die Erklärung von dem Signaturschlüssel-Inhaber abgegeben worden ist, streitet eine prima-facie-Vermutung für die Echtheit der Urkunde. Der Anschein der Echtheit kann vom Inhaber des Signaturschlüssels nur erschüttert werden, wenn er schlüssig Tatsachen vorträgt und beweist, die einen abweichenden Geschehensablauf ernsthaft als möglich erscheinen lassen.

§ 371a Abs. 2 S. 1 ZPO stellt den Beweiswert öffentlicher elektronischer Dokumente dem Beweiswert entsprechender öffentlicher Urkunden gleich. Durch diese Verweisung sind sowohl die allgemeinen Beweiskraftregeln in §§ 415, 417, 418 ZPO als auch die speziellen Vorschriften über die Beweiskraft des gerichtlichen Protokolls (§ 165 ZPO) und des Urteilstatbestands (§ 314 ZPO) erfasst. § 416a ZPO billigt dem Ausdruck eines öffentlichen elektronischen Dokuments die Wirkungen einer Urkunde zu, sofern der Ausdruck beglaubigt wird. Die Vorschrift ist nicht auf elektronische Dokumente anwendbar, die ursprünglich in Papierform vorgelegen haben und für die weitere Bearbeitung eingescannt worden sind.

## **7. Die elektronische Rechnung**

Rechnungen können – vorbehaltlich der Zustimmung des Empfängers – auch auf elektronischem Weg übermittelt werden, § 14 Abs. 1 S. 2 UStG.

Im steuerrechtlichen Bereich sind mit Blick auf die Erstellung und Übermittlung von elektronischen Rechnungen in den letzten Jahren grundlegende Veränderungen vorgenommen worden. War früher das Vorliegen einer Rechnung in Urkundenform, also als Schriftstück, zwingend notwendig, so wurde schon im Jahre 2002 mit der Einführung des § 14 Abs. 4 Satz 2 a.F. Umsatzsteuergesetz (UStG) die Möglichkeit geschaffen, Rechnungen mit einer qualifizierten elektronischen Signatur (ggf. mit Anbieter-Akkreditierung nach dem Signaturgesetz) versehen elektronisch zu übermitteln.

Das am 1.1.2004 in Kraft getretene Steueränderungsgesetz 2003 (StÄndG) sieht in dem neu gefassten § 14 Abs. 3 UStG – neben dieser Möglichkeit – vor, dass die für eine elektronische Übermittlung erforderliche Echtheit der Herkunft und die Unversehrtheit des Inhalts auch mittels elektronischen Datenaustauschs (EDI) gewährleistet werden können, wenn zusätzlich eine zusammenfassende Rechnung auf Papier oder auf elektronischem Weg mit qualifizierter elektronischer Signatur übermittelt wird. Nur eine auf diese Weise elektronisch übermittelte Rechnung berechtigt den Leistungsempfänger zum Vorsteuerabzug nach § 15 Abs. 1 Satz 1 Nr. 1 UStG.

Diese Regelungen zur elektronischen Rechnung hat das Bundesministerium der Finanzen mit Schreiben vom 29.1.2004 erläutert und insbesondere ausgeführt, dass das Signieren durch den Rechnungsaussteller auch in einem automatisierten Massenverfahren erfolgen kann. Es ist auch zulässig, mehrere Rechnungen in einer Datei zusammenzufassen und diese Datei mit nur einer qualifizierten elektronischen Signatur an den Empfänger zu übermitteln.

### **a. Zustimmung des Empfängers**

Für die elektronische Übermittlung von Rechnungen ist nach § 14 Abs. 1 S. 2 UStG die Zustimmung des Empfängers nötig. Diese Zustimmung bedarf keiner besonderen Form – es genügt, dass die Beteiligten die elektronische Übermittlung von Rechnungen tatsächlich praktizieren und damit stillschweigend billigen.

Grundsätzlich bietet sich eine entsprechende Klausel in den Allgemeinen Geschäftsbedingungen an.

#### **b. Elektronische Übermittlung durch Email**

Bei Übermittlung der Rechnung per E-Mail ist entsprechend § 14 Abs. 3 Nr. 1 UStG eine qualifizierte elektronische Signatur oder eine qualifizierte elektronische Signatur mit Anbieter-Akkreditierung entsprechend dem Signaturgesetz erforderlich, um die Echtheit der Herkunft und die Unversehrtheit der Daten zu gewährleisten.

#### **c. Die automatisierte elektronische Signatur**

Als automatisierte elektronische Signatur wird eine Signatur verstanden, die von einem automatischen Prozess ohne Zutun eines Menschen erzeugt wird. Dabei wird davon ausgegangen, dass ein Mensch diesen Prozess bewusst angestoßen hat, dass er aber weder die zu signierenden Daten im Einzelfall vor der Signatur überprüft noch den geheimen Schlüssel im Einzelfall freischaltet noch den Befehl zur Erzeugung der Signatur im Einzelfall gibt.

Die automatisierte elektronische Signatur ist unter bestimmten Umständen als qualifizierte elektronische Signatur anzuerkennen. Der Umstand, dass sie nicht durch persönliches Handeln des Signaturschlüsselinhabers, sondern durch einen von diesem initiierten und kontrollierten automatischen Prozess erzeugt worden ist, schließt diese Anerkennung nicht aus. Allerdings müssen auch für diese Form der Signaturerzeugung die Anforderungen des SigG und der SigV erfüllt werden.

#### **d. Dokumentation**

Der Aufbau und der Ablauf des bei der elektronischen Übermittlung einer Rechnung angewandten Verfahrens müssen für das Finanzamt innerhalb einer angemessenen Frist nachprüfbar sein, § 145 AO. Dies setzt eine Dokumentation voraus, dass das Verfahren den Anforderungen der Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) genügt (Anlage zum BMF-Schreiben vom 7.11.1995 – IV A 8 – S 0316 – 52/95). Das Bundesministerium der Finanzen hat in seinem Schreiben vom 16.07.2001 außerdem Grundsätze zum Datenzugriff, zur Prüfbarkeit digitaler Unterlagen und Archivierung digitaler Unterlagen fest gelegt (GDPdU), welche vorliegend zu beachten sind.

Fordert das Finanzamt den Unternehmer zur Vorlage der Rechnung auf, so ist nach den Grundsätzen der GDPdU nicht zu beanstanden, wenn der Unternehmer als vorläufigen Nachweis einen Ausdruck der elektronisch übermittelten Rechnung vorlegt.

Der Unternehmer muss jedoch auf Anforderung nachweisen, dass die elektronisch übermittelte Rechnung die Voraussetzungen des § 14 Abs. 3 UStG erfüllt.

#### **e. Die Aufbewahrung von elektronischen Rechnungen**

Absender und Empfänger der von elektronischen Rechnungen sind zur Aufbewahrung verpflichtet. Die Dokumente müssen während der Aufbewahrungsfrist nach den Grundsätzen der Ordnungsmäßigkeit an einem gesetzlich zulässigen Aufbewahrungsort aufbewahrt werden.

Nach § 14b Abs. 1 UStG hat der Unternehmer ein Doppel der Rechnung, die er selbst oder ein Dritter in seinem Namen und für seine Rechnung ausgestellt hat, sowie alle Rechnungen, die er erhalten oder die ein Leistungsempfänger oder in dessen Namen und für dessen Rechnung ein Dritter ausgestellt hat, zehn Jahre aufzubewahren.

Die Rechnungen müssen für den gesamten Zeitraum lesbar sein. Nachträgliche Änderungen sind nicht zulässig.

Bei elektronisch übermittelten Rechnungen hat der Unternehmer neben der Rechnung auch die Nachweise über die Echtheit und die Unversehrtheit der Daten aufzubewahren (z.B. qualifizierte elektronische Signatur), selbst wenn nach anderen Vorschriften die Gültigkeit dieser Nachweise bereits abgelaufen ist.

Es muss während der gesamten Aufbewahrungsfrist von originär digital erstellten Dokumenten sichergestellt sein, dass diese gem. § 147 Abs. 2 S. 1 Nr. 2 AO jederzeit unverzüglich lesbar gemacht und maschinell ausgewertet werden können.

#### **f. Inhaltliche Voraussetzungen der elektronischen Rechnung**

Die inhaltlichen Voraussetzungen der (elektronischen) Rechnung bestimmen sich nach § 14 Abs. 4 UStG,

wonach folgende Angaben enthalten sein müssen:

- der Name und die Anschrift des Rechnungsausstellers und des Rechnungsempfängers bzw. des Leistenden und des Leistungsempfängers,
- die Steuernummer oder die ihm vom Bundesamt für Finanzen erteilte Umsatzsteuer-Identifikationsnummer,
- das Ausstellungsdatum,
- die fortlaufende Rechnungsnummer,
- die Menge und die Art (handelsübliche Bezeichnung) der gelieferten Ware oder der Umfang und die Art der sonstigen Leistung,
- den Zeitpunkt der Lieferung oder sonstigen Leistung,
- das nach Steuersätzen und einzelnen Steuerbefreiungen aufgeschlüsselte Entgelt für die Lieferung oder sonstige Leistung einschließlich etwaiger Abzüge für Verrechnungen oder Rabatte etc.,
- den anzuwendenden Mehrwertsteuersatz und den darauf Steuerbetrag; ggf. Hinweis auf Steuerbefreiungen (Kleinunternehmen).

#### **g. Datenschutz**

Es bestehen keine datenschutzrechtlichen Bedenken gegenüber der Übertragung von Rechnungsdaten per Email. Grundsätzlich handelt es sich hierbei zwar (zumindest auch) um personenbezogene Daten, die nach § 4 BDSG nur erhoben, verarbeitet und genutzt werden, wenn die betroffene Person darin – grundsätzlich nach § 4a BDSG schriftlich – eingewilligt hat oder eine Rechtsnorm dies erlaubt. Nach § 28 Abs. 1 Nr. 2 BDSG ist die Verwendung personenbezogener Daten aber dann zulässig, wenn dies für die der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen, d.h. dem Rechnungsempfänger, dient. Dies ist bei der Rechnungsversendung per Email grundsätzlich der Fall.

#### **h. Elektronischer Datenaustausch (EDI-Rechnungen)**

Voraussetzung für die Anerkennung der im EDI-Verfahren nach § 14 Abs. 3 Nr. 2 UStG übermittelten Rechnungen ist, dass über den elektronischen Datenaustausch eine Vereinbarung nach Artikel 2 der Empfehlung 94/820/EG der Kommission vom 19. Oktober 1994 über die rechtlichen Aspekte des elektronischen Datenaustausches besteht,

in der der Einsatz von Verfahren vorgesehen ist, die die Echtheit der Herkunft und die Unversehrtheit der Daten gewährleisten.

Für mehrere getrennte Lieferungen von Gegenständen oder mehrere Dienstleistungen kann periodisch eine zusammenfassende Rechnung erstellt werden. Diese Rechnung muss für die einzelnen Umsätze eines Übertragungszeitraums die Entgelte und die darauf entfallenden Steuerbeträge jeweils in einer Summe zusammenfassen. Diese zusammenfassende Rechnung ist in Papierform oder in elektronischer Form, die mindestens mit einer qualifizierten elektronischen Signatur versehen wurde, dem Finanzamt einzureichen.

#### **i. Telefax-Rechnung**

Die Übermittlung von Rechnungen per Telefax ist im UStG nicht ausdrücklich geregelt. Nach dem Schreiben des Bundesfinanzministeriums vom 29. Januar 2004 gilt die Telefax-Rechnung als zulässige elektronische Übermittlung. Der Rechnungsaussteller muss einen Ausdruck in Papierform und der Rechnungsempfänger muss die eingehende Telefax-Rechnung in ausgedruckter Form aufbewahren.

Bei Telefax-Übertragungsformen, die nicht von Standard-Telefax an Standard-Telefax übermitteln, ist – wie bei der Rechnungsübermittlung per E-Mail – entsprechend § 14 Abs. 3 Nr. 1 UStG eine qualifizierte elektronische Signatur oder eine qualifizierte elektronische Signatur mit Anbieter-Akkreditierung erforderlich.

#### **j. Erstellung und elektronische Übermittlung von Rechnungen durch Dritte**

Auch für elektronisch übermittelte Rechnungen gilt, dass eine Rechnung im Namen und für Rechnung des Unternehmers oder eines in § 14 Abs. 2 S. 1 Nr. 2 UStG bezeichneten Leistungsempfängers von einem Dritten aufgestellt werden kann.

Bei der Einschaltung von Dritten werden eine oder mehrere natürliche Personen beim Dritten bevollmächtigt, für den leistenden Unternehmer oder im Falle der Gutschrift für den Leistungsempfänger Rechnungen mindestens mit einer qualifizierten elektronischen Signatur zu versehen.

### **8. Zusammenfassung**

Basierend auf einem komplizierten mathematischen Verfahren, ist die elektronische Signatur – vereinfacht ausgedrückt – ein digitales Siegel, welches bei der digitalen Übermittlung von Daten den Absender zweifelsfrei identifiziert und den Originalzustand der transportierten Daten gewährleistet.

Rechtlich relevant sind mit verschiedenen hohen Sicherheits-, Nachweis- und Kontrollniveaus: die fortgeschrittene elektronische Signatur, die qualifizierte elektronische Signatur und die qualifizierte elektronische Signatur mit Anbieter-Akkreditierung, § 2 SigG. Die gesetzliche Schriftform kann nur durch die qualifizierte elektronische Signatur (ggf. mit Anbieter-Akkreditierung) ersetzt werden, aber auch einfache und fortgeschrittene elektronische Signaturen können in einem gerichtlichen Prozess als Beweismittel eingesetzt werden. Auf elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, sind nach § 371a ZPO die Vorschriften über die Beweiskraft privater Urkunden entsprechend anwendbar, d.h. solche Dokumente werden wie (Papier-) Urkunden behandelt.

Nach § 14 Abs. 3 i. V. m. § 15 UStG berechtigen elektronisch erstellte Rechnungen, deren Echtheit der Herkunft und Unversehrtheit mit einer qualifizierten elektronischen Signatur (ggf. mit Anbieter-Akkreditierung) oder mittels elektronischen Datenaustauschs gewährleistet sind, zum Vorsteuerabzug. Für die elektronische Übermittlung ist jedoch gemäß § 14 Abs. 1 S.2 UStG die Zustimmung des Rechnungsempfängers nötig.

Bei elektronisch übermittelten Rechnungen hat der Unternehmer neben der Rechnung auch die Nachweise über die Echtheit und die Unversehrtheit der Daten aufzubewahren (z.B. qualifizierte elektronische Signatur), selbst wenn nach anderen Vorschriften die Gültigkeit dieser Nachweise bereits abgelaufen ist. Es ist dafür Sorge zu tragen, dass die elektronische Rechnung nebst Dokumentation der Signaturprüfung, Signaturprüfchlüssel, Zertifikat und ggf. weiterer Kryptographie-Schlüssel aufbewahrt wird.

\* \* \*