

**Die Regelung der  
elektronischen Kommunikation  
im  
Verwaltungsverfahrensgesetz**

11. Jahresarbeitstagung  
Verwaltungsrecht des DAI  
25./26. Februar 2005  
in Leipzig

**Die Regelung der elektronischen Kommunikation  
im Verwaltungsverfahrensgesetz**

**– Übersicht Material –**

1. *Thesen*
2. *Wie funktioniert die qualifizierte elektronische Signatur?*
3. *Gesetzestexte (Auszüge)*
4. *RdSchr. des BMI zur Amtlichen Beglaubigung (§§ 33, 34 VwVfG) v.  
1. 10. 2004 (= GMBI. 2005, 4)*

## **Die Regelung der elektronische Kommunikation im Verwaltungsverfahrensgesetz**

### **– Thesen –**

E-Mail-Verkehr ist selbstverständlicher Teil einer Büro-Einrichtung, im Einzelnen sind rechtliche Fragen zu dieser Technik noch offen.

Der Gesetzgeber hat rechtliche Rahmen für Zivil- und öffentliches Recht geschaffen. Für bestimmte Bereiche hat die Bundesregierung als Verordnungsgeber diese Rahmen durch nähere Regelungen zum elektronischen Rechtsverkehr ausgefüllt.

Praktische Fragen bleiben: Wie kann man am elektronischen Rechtsverkehr – insbesondere am elektronischen Verwaltungsverfahren – teilnehmen, welche Rechtswirkungen hat ein Verhalten im Einzelfall?

### **I. Elektronisches Verwaltungsverfahren**

„Elektronisches Verwaltungsverfahren“ reicht von einfacher Informationstätigkeit über Auskünfte (§ 25 Satz 2 VwVfG) bis zum Verwaltungsakt; es umfasst daneben auch inner- und zwischenbehördliches Handeln.

„E-Government“ bezeichnet ein strategisches Gesamtkonzept zur Modernisierung der Verwaltung mit Hilfe von IT-Technik: „Dienstleistungen“ der Verwaltung werden internetfähig gemacht, der Bürger erhält hierzu eine „Schnittstelle“. Ziel: das papierlose, rein elektronische Verwaltungshandeln.

### **1. Teilweise elektronisch abgewickeltes Verwaltungsverfahren**

IT-Technik in vielen Behörden **üblich** zur Unterstützung der Verwaltungstätigkeit: Fachinformation im behördeneigenen Intranet; Austausch von Informationen per e-Mail.

### **2. Vollständig elektronisch abgewickeltes Verwaltungsverfahren**

#### **Zielvorstellung:**

- a) Der Bürger sucht und findet allgemeine Informationen zu seinem Anliegen über die Homepage der Behörde. Ggfs. erhält er nähere Erläuterungen auf Anfrage durch e-Mail. Evtl. hat die Behörde erforderliche Formulare auf einem „Formularserver“ bereit gestellt.
- b) Antragstellung und Antragannahme interaktiv in diese Formulare. Alternativ: Antrag durch Zuleitung des am PC ausgefüllten Formulars oder formlos als e-Mail nebst eingescannter Anlagen an die Behörde.
- c) Prüfung des Antrags und evtl. eine weitere Sachverhaltsermittlung im „Workflow“ innerhalb der Behörde. Ggfs. erforderliche „Anhörung“ zu dem Ermittlungsergebnis durch Austausch von e-Mails. Entscheidung einschließlich etwaiger Mitwirkungshandlungen im behördlichen „Workflow“-System.
- d) Bekanntgabe der Entscheidung durch e-Mail in der Form des § 37 Abs. 2 bis 4 VwVfG.

## **II. Technische Grundlagen**

### **1. Verfahren der elektronischen Signatur**

Elektronische Signaturen: technische Verfahren, die gewährleisten, dass eine entsprechend signierte Nachricht von einem identifizierbaren Absender stammt und während der elektronischen Übermittlung zum Empfänger nicht verändert wurde.

## 2. *Unterschiedliche Qualitäten elektronischer Signaturen*

Nur bei **qualifizierten elektronischen Signaturen** ist auf Grund des durch das Signaturgesetz vorgegebenen Verfahrens eine zuverlässige Identitätsprüfung des Inhabers der Signaturkarte zwingend erforderlich und damit die notwendige Sicherheit für den Rechtsverkehr gegeben.

Neben den „qualifizierten“ Signaturen als mittlere Stufe sieht das neue Signaturgesetz „akkreditierte“ Signaturen (höchste Stufe) vor; daneben lässt es auch **sonstige Signaturen** (untere Stufe) zu. Diese sonstigen Signaturen sind jedoch nicht schriftformäquivalent i.S.v. § 126a Abs. 1 BGB und § 3a Abs. 2 VwVfG.

### III. **Rechtliche Grundlagen**

#### 1. *§ 3a VwVfG als Grundsatznorm*

Grundsätzlich ist das Verwaltungsverfahren nicht formgebunden; das schließt die Möglichkeit jeder Form elektronischer Kommunikation ein.

Durch Rechtsvorschrift angeordnete **Schriftform kann ersetzt werden** durch eine mit einer Signatur nach § 2 Nr. 3 SigG verbundene elektronische Form (**qualifizierte elektronische Form** – EU-Standard), § 3a Abs. 2 VwVfG.

#### 2. *Schriftformerfordernis*

Bei fachlich erforderlichen **Abweichungen** von der Grundsatznorm des § 3a VwVfG wird unterschieden:

- „nach unten“: Es bedarf bei elektronischer Kommunikation keiner besonderen Sicherheit. Ergänzung des die Schriftlichkeit anordnenden Gesetzestextes um die Worte „oder elektronisch“. Inhaltlich entspricht diese Kommunikationsweise dann der Textform des § 126b BGB.
- „nach oben“: Für bestimmte Verwaltungsakte sind zusätzliche Anforderungen an die qualifizierte elektronische Signatur zu stellen (§ 37 Abs. 4

VwVfG). Nennung der Anforderung im Gesetzestext („mit einer dauerhaft überprüfbaren Signatur nach § 37 Abs. 4 VwVfG“) oder allgemein durch Bezugnahme auf § 37 Abs. 4 VwVfG.

- „nicht elektronisch“: Ausschluss jeder Form elektronischer Kommunikation auszuschließen. Formulierungen wie „schriftlich, aber nicht in einer elektronischen Form“ oder „§ 3a VwVfG findet keine Anwendung“.

Wichtig: Nach dem Regelungsmechanismus der VwVfGe ist für Verfahren bei Landesbehörden das LVwVfG maßgebend. LVwVfGe übernehmen, wenn sie nicht dynamisch auf das des Bundes verweisen, dessen Änderungen in aller Regel wortgleich.

Auch jetzt haben die Bundesbestimmungen schon Wirkung für viele Verfahren der Länder, soweit Fachgesetze des Bundes Schriftlichkeit bestimmen. Was hier Schriftform ist, richtet sich nach § 3a Abs. 2 VwVfG.

§ 3a VwVfG ist – wie die Stellung im VwVfG vor den §§ 9 ff. zeigt – für die gesamte öffentlich-rechtliche Verwaltungstätigkeit anwendbar.

### **3. Zugangseröffnung durch den Empfänger**

Elektronische Kommunikation setzt Bereitschaft aller Verfahrensbeteiligten voraus: „Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet“ (§ 3a Abs. 1 VwVfG).

„Zugang“ stellt auf die objektiv vorhandene technische Kommunikationseinrichtung ab, also z.B. auf die Verfügbarkeit eines elektronischen Postfachs.

Das Erfordernis der „Eröffnung“ dieses Zugangs trägt den individuellen Möglichkeiten Rechnung. Der Empfänger eröffnet seinen Zugang durch entsprechende Widmung.

Widmung kann ausdrücklich oder konkludent erfolgen. Maßgebend ist hier die Verkehrsanschauung, die sich mit der Verbreitung elektronischer Kommunikationsmittel fortentwickelt.

Die **Behörde**, eine **Firma** oder ein **Rechtsanwalt**, die auf ihren Briefköpfen eine e-Mail-Adresse angeben, erklären damit konkludent ihre Bereitschaft,

Eingänge auf diesem Weg anzunehmen. Sie haben durch organisatorische Maßnahmen sicherzustellen, dass z.B. e-Mail-Postfächer regelmäßig abgefragt werden.

Gegenteiliges müssen die Betroffenen ausdrücklich erklären, z.B. durch Hinweise auf dem Briefkopf oder auf ihrer Internetseite.

Beim **Bürger** kann die bloße Angabe einer e-Mail-Adresse auf seinem Briefkopf heute noch nicht dahingehend verstanden werden, dass er damit seine Bereitschaft zum Empfang von rechtlich verbindlichen Erklärungen kundtut. Von der Eröffnung eines Zugangs kann nur ausgegangen werden, wenn er dies gegenüber der Behörde ausdrücklich erklärt hat. Dann zumindest starker indizieller Beweiswert der für e-Mail-Programme typischen Nachweise des e-Mail-Zugangs: „Übermittlungsbestätigung“ und „Lesebestätigung“.

Die automatisch generierte Lesebestätigung eines Empfängers, der keinen Zugang ausdrücklich für rechtsgeschäftliche Erklärungen geöffnet hat, begründet heute noch keinen Anscheinsbeweis für den Zugang der betreffenden e-Mail.

Der tatsächliche Umgang mit privaten PCs erlaubt weder die Annahme, dass der überwiegende Teil der Nutzer täglich seine Mailbox abfragt, noch die, dass eine generierte Lesebestätigung stets von dem Adressaten der e-Mail veranlasst worden ist.

#### **4. Störungen bei der elektronischen Kommunikation**

Grundsatz: **technische Kommunikationsprobleme gehen zu Lasten des Absenders.**

Aus § 3a Abs. 3 VwVfG ergeben sich jedoch Obliegenheiten für die Beteiligten, bei der Bewältigung solcher Probleme aktiv mitzuwirken.

Die Behörde hat bei Rüge des Empfängers, er könne das elektronische Dokument nicht bearbeiten, eine neue Übermittlung in geeigneter Form vorzunehmen.

Daraus folgt nicht generell, dass eine mangelhafte Übermittlung der elektronischen Daten keine Rechtsfolgen auszulösen vermag. Solange der **Inhalt**

der Mitteilung **eindeutig zu erkennen** ist, werden der **Zugang** und evtl. Fristsetzungen nicht beeinträchtigt. § 3a Abs. 3 VwVfG trifft insoweit keine Regelung über den Zugang von elektronischen Dokumenten; dieser bestimmt sich vielmehr nach den allgemeinen Grundsätzen.

Ein gar nicht oder in wesentlichen Teilen **nicht lesbares Dokument** ist **nicht zugegangen**. Die Behörde ist zur erneuten Übermittlung in geeigneter Form aber auch dann verpflichtet, wenn das Dokument trotz fehlerbehafteter elektronischer Übermittlung zugegangen, da der Begriff „Bearbeitung“ in § 3a Abs. 3 VwVfG weit zu verstehen ist.

Die allgemeinen Grundsätze, insb. hinsichtlich der Wahrung von Fristen, gelten ebenfalls bei der elektronischen Übermittlung vom Bürger zur Verwaltung. Die Behörde hat im Rahmen des durch die Kommunikation entstandenen Verwaltungsrechtsverhältnisses bei Kommunikationsproblemen dem Bürger unverzüglich (§ 122 Abs. 1 Satz 1 BGB) die notwendigen Informationen – z.B. über ein von ihr lesbares Textformat – zu geben (§ 3a Abs. 3 Satz 1 VwVfG).

Zu unterscheiden von Fehlern durch die Kommunikationstechnik sind inhaltliche Fehler bei Verwaltungsakten. Die Berichtigungsmöglichkeiten nach § 42 VwVfG erfassen auch offenbare Unrichtigkeiten in einem elektronischen Dokument.

## 5. *Die elektronische Akte*

Die **Funktionen der schriftlichen Akte**, den Geschehensablauf wahrheitsgetreu und vollständig zu dokumentieren, müssen **auch für die bei der elektronischen Vorgangsbearbeitung anfallenden Dateien** sichergestellt werden.

Vom Beginn des Verfahrens bis zur Archivierung sind von der Verwaltung alle wesentlichen Arbeitsschritte sicher, also gegen nachträgliche Manipulation geschützt, festzuhalten.

Nach Erlass der Rechtsverordnungen i.S.v. § 86a Abs. 2 VwGO ist im Verkehr mit dem BVerwG nun die Übermittlung von Akten und Schriftsätzen auch in elektronischer Form möglich.

Verkehr mit den Gerichten im Übrigen: Bis zu einer technischen Reife, die es den Gerichten ermöglicht, unmittelbar die elektronischen Daten eines Verwaltungsverfahrens – durch vollständige Übertragung des einschlägigen Datenbestands an das Gericht oder vielleicht später auch durch Eröffnung einer Zugriffsmöglichkeit über das Internet – einzusehen, kommt zunächst in Betracht, für das Gerichtsverfahren alle Dateien auszudrucken und deren Authentizität und Vollständigkeit **amtlich zu beglaubigen**, § 33 VwVfG.

Im Verwaltungsverfahren sind elektronische Dokumente geeignete Beweismittel i.S.d. § 26 VwVfG. Die Aufzählung der Beweismittel in den Nummern 1 bis 4 ist nicht abschließend. Gleichwohl ist bei der Nutzung der elektronischen Form zu berücksichtigen, dass diese rechtlich wirksam nur erhalten bleibt, solange sie auf einem elektronischen Speichermedium vorgehalten wird. Der Ausdruck eines elektronischen Verwaltungsaktes erhält erst durch eine Beglaubigung wieder einen der elektronischen Form entsprechenden rechtlichen Wert; ohne diese ist er lediglich Beweiszeichen für den Inhalt des entsprechenden elektronischen Verwaltungsaktes.

## **6.     *Datenschutz***

Die Behörde muss, wie in § 30 VwVfG vorgesehen, die notwendigen Sicherheitsvorkehrungen treffen, also etwa elektronische Dokumente zum **Schutz gegen unbefugte Kenntnisnahme** in geeigneter Weise verschlüsseln.

# **IV.   Elektronische Verwaltung in der aktuellen Praxis**

## **1.     *Binnenkommunikation der Verwaltung***

Papier- und Telefaxverkehr werden zunehmend von e-Mail-Verkehr ersetzt oder begleitet.

## **2.     *Verkehr mit dem Bürger***

Im Verkehr mit dem Bürger sind die praktischen Erfahrungen noch geringer: Stand der technischen Ausrüstung des Bürgers.

Die Entwicklung des elektronischen Verkehrs von Behörden und „Normal“-Bürger wird die entsprechende Veränderung der „Verwaltungskultur“ voraussetzen. Die Verwaltung muss hierzu aktiv werden und Angebote machen.

In absehbarer Zeit ist **kein Verzicht auf herkömmliche Kommunikationsmittel** denkbar. Der Kontakt mit der Verwaltung ist in der Lebenswirklichkeit des normalen Bürgers randständig. Vielfach wird eine elektronische Kommunikation gar nicht gewünscht sein: Ein Bauwilliger wird z.B. den persönlichen Kontakt zu dem Sachbearbeiter in der Behörde suchen, um im Gespräch seine Möglichkeiten zu eruieren und ggfs. eine Verhandlungslösung zu erzielen.

Für nicht absehbare Zeit wird ein großer Teil der Bevölkerung keinen Zugang zu der für elektronische Kommunikation erforderlichen Technik haben.

## **3.     *Informationstätigkeit der Behörden***

Aktive Information durch die Behörden dient der Verwaltungsvereinfachung, da sie die individuelle Bearbeitung von Informationsanträgen reduziert.

# Wie funktioniert die qualifizierte elektronische Signatur?

Eine digitale Signatur im Sinne des Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Signaturschlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt. Vor allem vier Eigenschaften für eine sichere Kommunikation sollen durch den Einsatz von digitalen Signaturen erfüllt werden:

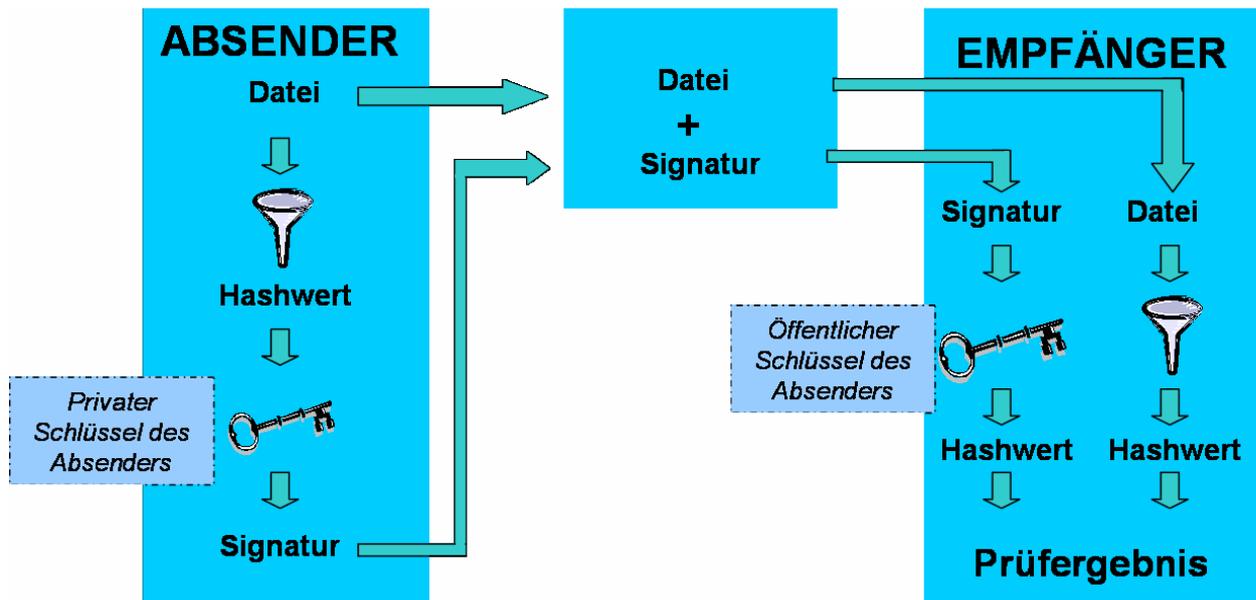
- Authentizität (die Herkunft der Daten muss nachweisbar sein),
- Integrität (die ausgetauschten Daten haben nur Gültigkeit, wenn der Inhalt sowie die angeführten Adressen unversehrt sind),
- Vertraulichkeit (die Daten sind vor der Einsicht durch Unbefugte geschützt),
- Verbindlichkeit (der Absender kann nicht leugnen, die Nachricht selbst versendet zu haben).

## I.

### Verwendung der qualifizierten elektronischen Signatur

Der Absender A verfügt über ein erforderliches Schlüsselpaar. Die jeweils einmaligen Schlüsselpaare (privater und öffentlicher Schlüssel, die mathematisch voneinander abhängen) werden durch staatlich anerkannte Stellen natürlichen Personen fest zugeordnet. Die Zuordnung wird durch ein qualifiziertes Signaturschlüssel-Zertifikat beglaubigt. Es handelt sich dabei um ein signiertes digitales Dokument, das den jeweiligen öffentlichen Schlüssel sowie den Namen der Person, der er zugeordnet ist, oder ein Pseudonym enthält. Das Zertifikat erhält der Signaturschlüssel-Inhaber, so dass er es signierten Daten für deren Überprüfung beifügen kann. Darüber hinaus ist es über öffentlich erreichbare Telekommunikationsverbindungen (z. B. Internet) jederzeit für jedermann nachprüfbar. Die einzelnen Schritte:

- A erstellt ein Dokument und klickt auf den Knopf „Signieren“. Der PC bildet eine Prüfsumme (Hashwert) aus dem Dokument und fordert die Verschlüsselung mit dem privaten Schlüssel von A bei dessen Chipkarte an.
- A steckt die Chipkarte mit seinem Schlüsselzertifikat in das an den PC angeschlossene Lesegerät. Die Chipkarte fordert die Freigabe der Aktion durch die zugehörige PIN von A.
- A gibt seine PIN ein. Die Chipkarte überprüft die PIN, verschlüsselt (signiert) die Prüfsumme (Hashwert) und überträgt diese zum PC. Der PC setzt die Signatur unter das Dokument.
- Das Dokument wird mit Signatur versandt.
- Der Empfänger E entschlüsselt die empfangene Signatur mit Hilfe des öffentlichen Schlüssels von A. Der PC von E vergleicht dann die Signatur mit dem ebenfalls auf eine Prüfsumme (Hashwert) reduzierten empfangenen Dokument. Stimmen die entschlüsselte Signatur und die Prüfsumme überein, ist das Dokument unverfälscht und kann nur vom Inhaber des Schlüsselzertifikats A stammen.



## II.

**Mathematisch sieht die Prozedur wie folgt aus:**

- $K_A$  A's öffentlicher Schlüssel
- $K_A^{-1}$  A's geheimer Schlüssel
- $\{x\}_K$  Verschlüsselung von  $x$  mit dem Schlüssel  $K$
- $N$  eine Nachricht
- $h(N)$  Hashwert der Nachricht
- $S$  Signatur

Möchte A nun eine Nachricht  $N$  für E unterschreiben, bildet er den Hashwert  $h(N)$  der Nachricht. Dieser ist eine Prüfsumme aus den Daten der Nachricht; ändert sich ein Bit der Nachricht, so ist mit extrem hoher Wahrscheinlichkeit der Hashwert ein anderer. Um eine Signatur  $S$  zu erhalten, verschlüsselt A diesen Hashwert mit seinem geheimen (!) Schlüssel.

$$S = \{h(N)\}_{K_A^{-1}}$$

Bei der Verschlüsselung geht es nicht darum, den Inhalt des Hashwertes zu verbergen, sondern es soll sichergestellt werden, dass E die Signatur mit dem öffentlichen Schlüssel von A (und zwar nur mit dem von A) wieder entschlüsseln kann.

Nun sendet A die Nachricht  $N$  und die Signatur  $S$  an E. Dieser berechnet nun seinerseits den Hashwert  $h(N)$  aus der Nachricht  $N$ . Nun wendet er A's öffentlichen Schlüssel auf die Signatur an

$$h' = \{S\}_{K_A}$$

und macht somit A's Verschlüsselung rückgängig. Nun muss E nur noch vergleichen ob

$$h' = h(N)$$

um zu wissen, dass A das Dokument unterschrieben hat. E stellt dabei fest, dass der Hashwert korrekt mit einem Schlüssel verschlüsselt wurde, den nur A kennen konnte. Darum weiß er, dass das Dokument von A signiert wurde. Sollte  $h'$  ungleich  $h(N)$  sein, so ist das Dokument entweder unterwegs verfälscht worden (Nachweis der Integrität) oder nicht mit dem Schlüssel von A signiert worden (Nachweis der Authentizität). Diese Abläufe und Berechnungen werden von entsprechenden Programmen automatisch vorgenommen.

In zertifikatsbasierten Systemen erhält jeder Benutzer ein digitales Zertifikat, das seine Identität beschreibt und die öffentlichen Schlüssel enthält. Jedes Zertifikat ist von einer ausgebenden Stelle beglaubigt, die ihrerseits wieder von höheren Stellen beglaubigt sein kann. Das Vertrauenssystem ist streng hierarchisch. Den gemeinsamen Vertrauensanker bildet ein sog. Wurzel-Zertifikat (Root Certificate).

Ein Zertifikat verknüpft Daten eines kryptographischen Schlüssels (oder Schlüsselpaars, bestehend aus öffentlichem und privatem Schlüssel) mit Daten des Inhabers und einer Zertifizierungsstelle, sowie weitere Spezifikationen wie Version, Gültigkeitsdauer und Verwendungszweck.

Beim Web-Datenaustausch überträgt der Server seinen öffentlichen Schlüssel an den Client. Der Client, d.i. der Webbrowser des Nutzers, überlegt, ob er dem öffentlichen Schlüssel trauen kann. Dazu schaut er in die Liste seiner Zertifikate, die ihm bei der Installation mitgegeben wurden oder der Benutzer selbst installiert hat. Findet er dort das Zertifikat, startet er eine verschlüsselte Datenübertragung. Neue Zertifikate kann der Benutzer über das Internet beim Herausgeber überprüfen.

### III.

#### **Zertifizierungsstelle (Trustcenter)**

Trustcenter gewährleisten die allgemeine Sicherheit einer Public-Key Infrastruktur (PKI) und stellen die zentralen Institutionen des Vertrauens dar, indem sie eine verbindliche dedizierte Zuordnung von Schlüsselpaaren zu Personen vornehmen (Zertifizierung).

Das System der elektronischen Signatur kann ohne Trustcenter nicht funktionieren. Es muss eine Stelle existieren, die das Schlüsselpaar für die Signaturkarte in einer sicheren Umgebung erstellt und insbesondere die Zuordnung einer Person zu einem Schlüsselpaar feststellt und für die anderen Teilnehmer bescheinigt.

Die Bescheinigung dieser Zuordnung einer Person zu einem Schlüssel wird von einer Zertifizierungsstelle durchgeführt. Wichtig für das System der elektronischen Signaturen ist das Vorhandensein von Institutionen, die eine verbindliche Zuordnung eines Schlüsselpaars zu einer Person vornehmen. Den Teilnehmern einer elektronischen Kommunikation ohne zusätzliche Sicherungsmittel fehlt das Vertrauen in die Identität des Anderen und in die Integrität der übermittelten Inhalte. Die Aufgabe, dieses Vertrauen zwischen den Beteiligten einer elektronischen Kommunikation herzustellen, wird im System der elektronischen Signatur von den Trustcentern wahrgenommen.

Zertifizierung bedeutet wörtlich genommen "Bescheinigung". Trustcenter bescheinigen somit, dass ein öffentlicher Schlüssel zu dem Eigentümer des Schlüsselpaares gehört. Um diese Zuordnung von Schlüssel und Eigentümer leisten zu können, stellen Trustcenter die Identität ihrer Kunden zuverlässig fest. Erst nachdem das Trustcenter die Identität des Kunden zweifelsfrei festgestellt hat, erstellt es individuell für den Kunden eine Signaturkarte mit den entsprechenden Zertifikaten.

Trustcenter sind mit einem erheblichen sicherheitstechnischem Aufwand in speziellen Bunkerräumen untergebracht. Umfangreiche technische und bauliche Maßnahmen machen einen unbefugten Zugriff auf die Räume dieses Bereichs unmöglich. Alle elektronischen Zugänge sind mehrfach und ausfallsicher ausgelegt. Die Räume können nur durch Vereinzelungsschleusen von ausgewählten Mitarbeitern ausschließlich für die notwendigen Arbeitsschritte betreten werden. Alle Mitarbeiter unterliegen einer ständigen Sicherheitsüberprüfung. Auf diese Weise wird die Einhaltung der gesetzlichen Rahmenbedingungen für die elektronische Signatur garantiert.

**Die Regelung der elektronischen Kommunikation  
im Verwaltungsverfahrensgesetz**

**Gesetzestexte**

**BGB**

§§ 121, 126, 126a, 126b - 2 -

**VwVfG**

§§ 3a, 9, 10, 24, 25, 26, 30, 33, 34, 37, 42 - 4 -

**SigG**

§ 2 - 11 -

**ZPO**

§§ 292a, 371a (Entwurf) - 13 -

**VwGO**

§§ 70, 86a, 96, 99 - 14 -

**GBO**

§ 126 - 17 -

## **BGB**

### **§ 121**

(1) Die Anfechtung muss in den Fällen der §§ 119, 120 ohne schuldhaftes Zögern (unverzüglich) erfolgen, nachdem der Anfechtungsberechtigte von dem Anfechtungsgrund Kenntnis erlangt hat. Die einem Abwesenden gegenüber erfolgte Anfechtung gilt als rechtzeitig erfolgt, wenn die Anfechtungserklärung unverzüglich abgesendet worden ist.

(2) Die Anfechtung ist ausgeschlossen, wenn seit der Abgabe der Willenserklärung zehn Jahre verstrichen sind.

### **§ 126**

(1) Ist durch Gesetz schriftliche Form vorgeschrieben, so muss die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden.

(2) Bei einem Vertrag muss die Unterzeichnung der Parteien auf derselben Urkunde erfolgen. Werden über den Vertrag mehrere gleichlautende Urkunden aufgenommen, so genügt es, wenn jede Partei die für die andere Partei bestimmte Urkunde unterzeichnet.

(3) Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt.

(4) Die schriftliche Form wird durch die notarielle Beurkundung ersetzt.

### **§ 126a**

(1) Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.

(2) Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument in der in Absatz 1 bezeichneten Weise elektronisch signieren.

### **§ 126b**

Ist durch Gesetz Textform vorgeschrieben, so muss die Erklärung in einer Urkunde oder auf andere zur dauerhaften Wiedergabe in Schriftzeichen geeignete Weise abgegeben, die Person des Erklärenden genannt und der Abschluss der Erklärung durch Nachbildung der Namensunterschrift oder anders erkennbar gemacht werden.

## **VwVfG**

### **§ 3a**

#### **Elektronische Kommunikation**

(1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.

(2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, ist nicht zulässig.

(3) Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, hat sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück zu übermitteln.

### **§ 9**

#### **Begriff des Verwaltungsverfahrens**

Das Verwaltungsverfahren im Sinne dieses Gesetzes ist die nach außen wirkende Tätigkeit der Behörden, die auf die Prüfung der Voraussetzungen, die Vorbereitung und den Erlass eines Verwaltungsaktes oder auf den Abschluss eines öffentlich-rechtlichen Vertrags gerichtet ist; es schließt den Erlass des Verwaltungsaktes oder den Abschluss des öffentlich-rechtlichen Vertrags ein.

## **§ 10**

### **Nichtförmlichkeit des Verfahrens**

Das Verwaltungsverfahren ist an bestimmte Formen nicht gebunden, soweit keine besonderen Rechtsvorschriften für die Form des Verfahrens bestehen. Es ist einfach, zweckmäßig und zügig durchzuführen.

## **§ 24**

### **Untersuchungsgrundsatz**

(1) Die Behörde ermittelt den Sachverhalt von Amts wegen. Sie bestimmt Art und Umfang der Ermittlungen; an das Vorbringen und an die Beweisanträge der Beteiligten ist sie nicht gebunden.

(2) Die Behörde hat alle für den Einzelfall bedeutsamen, auch die für die Beteiligten günstigen Umstände zu berücksichtigen.

(3) Die Behörde darf die Entgegennahme von Erklärungen oder Anträgen, die in ihren Zuständigkeitsbereich fallen, nicht deshalb verweigern, weil sie die Erklärung oder den Antrag in der Sache für unzulässig oder unbegründet hält.

## **§ 25**

### **Beratung, Auskunft**

Die Behörde soll die Abgabe von Erklärungen, die Stellung von Anträgen oder die Berichtigung von Erklärungen oder Anträgen anregen, wenn diese offensichtlich nur versehentlich oder aus Unkenntnis unterblieben oder unrichtig abgegeben oder gestellt worden sind. Sie erteilt, soweit erforderlich, Auskunft über die den Beteiligten im Verwaltungsverfahren zustehenden Rechte und die ihnen obliegenden Pflichten.

## **§ 26**

### **Beweismittel**

(1) Die Behörde bedient sich der Beweismittel, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält. Sie kann insbesondere

1. Auskünfte jeder Art einholen,
2. Beteiligte anhören, Zeugen und Sachverständige vernehmen oder die schriftliche oder elektronische Äußerung von Beteiligten, Sachverständigen und Zeugen einholen,
3. Urkunden und Akten beiziehen,
4. den Augenschein einnehmen.

(2) Die Beteiligten sollen bei der Ermittlung des Sachverhalts mitwirken. Sie sollen insbesondere ihnen bekannte Tatsachen und Beweismittel angeben. Eine weitergehende Pflicht, bei der Ermittlung des Sachverhalts mitzuwirken, insbesondere eine Pflicht zum persönlichen Erscheinen oder zur Aussage, besteht nur, soweit sie durch Rechtsvorschrift besonders vorgesehen ist.

(3) Für Zeugen und Sachverständige besteht eine Pflicht zur Aussage oder zur Erstattung von Gutachten, wenn sie durch Rechtsvorschrift vorgesehen ist. Falls die Behörde Zeugen und Sachverständige herangezogen hat, erhalten sie auf Antrag in entsprechender Anwendung des Justizvergütungs- und -entschädigungsgesetzes eine Entschädigung oder Vergütung.

## **§ 30**

### **Geheimhaltung**

Die Beteiligten haben Anspruch darauf, dass ihre Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse sowie die Betriebs- und Geschäftsgeheimnisse, von der Behörde nicht unbefugt offenbart werden.

## **§ 33**

### **Beglaubigung von Dokumenten**

(1) Jede Behörde ist befugt, Abschriften von Urkunden, die sie selbst ausgestellt hat, zu beglaubigen. Darüber hinaus sind die von der Bundesregierung durch

Rechtsverordnung bestimmten Behörden im Sinne des § 1 Abs. 1 Nr. 1 und die nach Landesrecht zuständigen Behörden befugt, Abschriften zu beglaubigen, wenn die Urschrift von einer Behörde ausgestellt ist oder die Abschrift zur Vorlage bei einer Behörde benötigt wird, sofern nicht durch Rechtsvorschrift die Erteilung beglaubigter Abschriften aus amtlichen Registern und Archiven anderen Behörden ausschließlich vorbehalten ist; die Rechtsverordnung bedarf nicht der Zustimmung des Bundesrates.

(2) Abschriften dürfen nicht beglaubigt werden, wenn Umstände zu der Annahme berechtigen, dass der ursprüngliche Inhalt des Schriftstücks, dessen Abschrift beglaubigt werden soll, geändert worden ist, insbesondere wenn dieses Schriftstück Lücken, Durchstreichungen, Einschaltungen, Änderungen, unleserliche Wörter, Zahlen oder Zeichen, Spuren der Beseitigung von Wörtern, Zahlen und Zeichen enthält oder wenn der Zusammenhang eines aus mehreren Blättern bestehenden Schriftstücks aufgehoben ist.

(3) Eine Abschrift wird beglaubigt durch einen Beglaubigungsvermerk, der unter die Abschrift zu setzen ist. Der Vermerk muss enthalten

1. die genaue Bezeichnung des Schriftstücks, dessen Abschrift beglaubigt wird,
2. die Feststellung, dass die beglaubigte Abschrift mit dem vorgelegten Schriftstück übereinstimmt,
3. den Hinweis, dass die beglaubigte Abschrift nur zur Vorlage bei der angegebenen Behörde erteilt wird, wenn die Urschrift nicht von einer Behörde ausgestellt worden ist,
4. den Ort und den Tag der Beglaubigung, die Unterschrift des für die Beglaubigung zuständigen Bediensteten und das Dienstsiegel.

(4) Die Absätze 1 bis 3 gelten entsprechend für die Beglaubigung von

1. Ablichtungen, Lichtdrucken und ähnlichen in technischen Verfahren hergestellten Vervielfältigungen,
2. auf fototechnischem Wege von Schriftstücken hergestellten Negativen, die bei einer Behörde aufbewahrt werden,
3. Ausdrucken elektronischer Dokumente,
4. elektronischen Dokumenten,
  - a) die zur Abbildung eines Schriftstücks hergestellt wurden,
  - b) die ein anderes technisches Format als das mit einer qualifizierten elektronischen Signatur verbundene Ausgangsdokument erhalten haben.

(5) Der Beglaubigungsvermerk muss zusätzlich zu den Angaben nach Absatz 3 Satz 2 bei der Beglaubigung

1. des Ausdrucks eines elektronischen Dokuments, das mit einer qualifizierten elektronischen Signatur verbunden ist, die Feststellungen enthalten,
  - a) wen die Signaturprüfung als Inhaber der Signatur ausweist,
  - b) welchen Zeitpunkt die Signaturprüfung für die Anbringung der Signatur ausweist und
  - c) welche Zertifikate mit welchen Daten dieser Signatur zugrunde lagen;
2. eines elektronischen Dokuments den Namen des für die Beglaubigung zuständigen Bediensteten und die Bezeichnung der Behörde, die die Beglaubigung vornimmt, enthalten; die Unterschrift des für die Beglaubigung zuständigen Bediensteten und das Dienstsiegel nach Absatz 3 Satz 2 Nr. 4 werden durch eine dauerhaft überprüfbare qualifizierte elektronische Signatur ersetzt.

Wird ein elektronisches Dokument, das ein anderes technisches Format als das mit einer qualifizierten elektronischen Signatur verbundene Ausgangsdokument erhalten hat, nach Satz 1 Nr. 2 beglaubigt, muss der Beglaubigungsvermerk zusätzlich die Feststellungen nach Satz 1 Nr. 1 für das Ausgangsdokument enthalten.

(6) Die nach Absatz 4 hergestellten Dokumente stehen, sofern sie beglaubigt sind, beglaubigten Abschriften gleich.

## **§ 34**

### **Beglaubigung von Unterschriften**

(1) Die von der Bundesregierung durch Rechtsverordnung bestimmten Behörden im Sinne des § 1 Abs. 1 Nr. 1 und die nach Landesrecht zuständigen Behörden sind befugt, Unterschriften zu beglaubigen, wenn das unterzeichnete Schriftstück zur Vorlage bei einer Behörde oder bei einer sonstigen Stelle, der auf Grund einer Rechtsvorschrift das unterzeichnete Schriftstück vorzulegen ist, benötigt wird. Dies gilt nicht für

1. Unterschriften ohne zugehörigen Text,
2. Unterschriften, die der öffentlichen Beglaubigung (§ 129 des Bürgerlichen Gesetzbuchs) bedürfen.

(2) Eine Unterschrift soll nur beglaubigt werden, wenn sie in Gegenwart des beglaubigenden Bediensteten vollzogen oder anerkannt wird.

(3) Der Beglaubigungsvermerk ist unmittelbar bei der Unterschrift, die beglaubigt werden soll, anzubringen. Er muss enthalten

1. die Bestätigung, dass die Unterschrift echt ist,
2. die genaue Bezeichnung desjenigen, dessen Unterschrift beglaubigt wird, sowie die Angabe, ob sich der für die Beglaubigung zuständige Bedienstete Gewissheit über diese Person verschafft hat und ob die Unterschrift in seiner Gegenwart vollzogen oder anerkannt worden ist,
3. den Hinweis, dass die Beglaubigung nur zur Vorlage bei der angegebenen Behörde oder Stelle bestimmt ist,
4. den Ort und den Tag der Beglaubigung, die Unterschrift des für die Beglaubigung zuständigen Bediensteten und das Dienstsiegel.

(4) Die Absätze 1 bis 3 gelten für die Beglaubigung von Handzeichen entsprechend.

(5) Die Rechtsverordnungen nach Absatz 1 und 4 bedürfen nicht der Zustimmung des Bundesrates.

## **§ 37**

### **Bestimmtheit und Form des Verwaltungsaktes**

(1) Ein Verwaltungsakt muss inhaltlich hinreichend bestimmt sein.

(2) Ein Verwaltungsakt kann schriftlich, elektronisch, mündlich oder in anderer Weise erlassen werden. Ein mündlicher Verwaltungsakt ist schriftlich oder elektronisch zu bestätigen, wenn hieran ein berechtigtes Interesse besteht und der Betroffene dies unverzüglich verlangt. Ein elektronischer Verwaltungsakt ist unter denselben Voraussetzungen schriftlich zu bestätigen; § 3a Abs. 2 findet insoweit keine Anwendung.

(3) Ein schriftlicher oder elektronischer Verwaltungsakt muss die erlassende Behörde erkennen lassen und die Unterschrift oder die Namenswiedergabe des Behördenleiters, seines Vertreters oder seines Beauftragten enthalten. Wird für einen Verwaltungsakt, für den durch Rechtsvorschrift die Schriftform angeordnet ist, die elektronische Form verwendet, muss auch das der Signatur zugrunde liegende qualifizierte Zertifikat oder ein zugehöriges qualifiziertes Attributzertifikat die erlassende Behörde erkennen lassen.

(4) Für einen Verwaltungsakt kann für die nach § 3a Abs. 2 erforderliche Signatur durch Rechtsvorschrift die dauerhafte Überprüfbarkeit vorgeschrieben werden.

(5) Bei einem schriftlichen Verwaltungsakt, der mit Hilfe automatischer Einrichtungen erlassen wird, können abweichend von Absatz 3 Unterschrift und Namenswiedergabe fehlen. Zur Inhaltsangabe können Schlüsselzeichen verwendet werden, wenn derjenige, für den der Verwaltungsakt bestimmt ist oder der von ihm betroffen wird, auf Grund der dazu gegebenen Erläuterungen den Inhalt des Verwaltungsaktes eindeutig erkennen kann.

## **§ 42**

### **Offenbare Unrichtigkeiten im Verwaltungsakt**

Die Behörde kann Schreibfehler, Rechenfehler und ähnliche offenbare Unrichtigkeiten in einem Verwaltungsakt jederzeit berichtigen. Bei berechtigtem Interesse des Beteiligten ist zu berichtigen. Die Behörde ist berechtigt, die Vorlage des Dokuments zu verlangen, das berichtigt werden soll.

## **SigG**

### **§ 2**

#### **Begriffsbestimmungen**

Im Sinne dieses Gesetzes sind

1. "elektronische Signaturen" Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,
2. "fortgeschrittene elektronische Signaturen" elektronische Signaturen nach Nummer 1, die
  - a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
  - b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
  - c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
  - d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,
3. "qualifizierte elektronische Signaturen" elektronische Signaturen nach Nummer 2, die
  - a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
  - b) mit einer sicheren Signaturerstellungseinheit erzeugt werden,
4. "Signaturschlüssel" einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden,
5. "Signaturprüf Schlüssel" elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden,
6. "Zertifikate" elektronische Bescheinigungen, mit denen Signaturprüf Schlüssel einer Person zugeordnet werden und die Identität dieser Person bestätigt wird,
7. "qualifizierte Zertifikate" elektronische Bescheinigungen nach Nummer 6 für natürliche Personen, die die Voraussetzungen des § 7 erfüllen und von Zertifizierungsdiensteanbietern ausgestellt werden, die mindestens die Anforderungen nach den §§ 4 bis 14 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllen,
8. "Zertifizierungsdiensteanbieter" natürliche oder juristische Personen, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen,

9. "Signaturschlüssel-Inhaber" natürliche Personen, die Signaturschlüssel besitzen; bei qualifizierten elektronischen Signaturen müssen ihnen die zugehörigen Signaturprüfchlüssel durch qualifizierte Zertifikate zugeordnet sein,
10. "sichere Signaturerstellungseinheiten" Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, die mindestens die Anforderungen nach § 17 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllen und die für qualifizierte elektronische Signaturen bestimmt sind,
11. "Signaturanwendungskomponenten" Software- und Hardwareprodukte, die dazu bestimmt sind,
  - a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder
  - b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen,
12. "technische Komponenten für Zertifizierungsdienste" Software- oder Hardwareprodukte, die dazu bestimmt sind,
  - a) Signaturschlüssel zu erzeugen und in eine sichere Signaturerstellungseinheit zu übertragen,
  - b) qualifizierte Zertifikate öffentlich nachprüfbar und gegebenenfalls abrufbar zu halten oder
  - c) qualifizierte Zeitstempel zu erzeugen,
13. "Produkte für qualifizierte elektronische Signaturen" sichere Signaturerstellungseinheiten, Signaturanwendungskomponenten und technische Komponenten für Zertifizierungsdienste,
14. "qualifizierte Zeitstempel" elektronische Bescheinigungen eines Zertifizierungsdiensteanbieters, der mindestens die Anforderungen nach den §§ 4 bis 14 sowie § 17 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllt, darüber, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben,
15. "freiwillige Akkreditierung" Verfahren zur Erteilung einer Erlaubnis für den Betrieb eines Zertifizierungsdienstes, mit der besondere Rechte und Pflichten verbunden sind.

## **ZPO**

### **§ 292a**

#### **Anscheinsbeweis bei qualifizierter elektronischer Signatur**

Der Anschein der Echtheit einer in elektronischer Form (§ 126a des Bürgerlichen Gesetzbuchs) vorliegenden Willenserklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen; dass die Erklärung mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist.

### **§ 371a (Entwurf)**

#### **Beweiskraft elektronischer Dokumente**

(1) Auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.

(2) Auf elektronische Dokumente, die von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind (öffentliche elektronische Dokumente), finden die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Ist das Dokument mit einer qualifizierten elektronischen Signatur versehen, gilt § 437 entsprechend.

## **VwGO**

### **§ 70**

(1) Der Widerspruch ist innerhalb eines Monats, nachdem der Verwaltungsakt dem Beschwerdeführer bekanntgegeben worden ist, schriftlich oder zur Niederschrift bei der Behörde zu erheben, die den Verwaltungsakt erlassen hat. Die Frist wird auch durch Einlegung bei der Behörde, die den Widerspruchsbescheid zu erlassen hat, gewahrt.

(2) §§ 58 und 60 Abs. 1 bis 4 gelten entsprechend.

### **§ 86a**

(1) Soweit für vorbereitende Schriftsätze und deren Anlagen, für Anträge und Erklärungen der Parteien sowie für Auskünfte, Aussagen, Gutachten und Erklärungen Dritter die Schriftform vorgesehen ist, genügt dieser Form die Aufzeichnung als elektronisches Dokument, wenn dieses für die Bearbeitung durch das Gericht geeignet ist. Die verantwortende Person soll das Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen.

(2) Die Bundesregierung und die Landesregierungen bestimmen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können, sowie die für die Bearbeitung der Dokumente geeignete Form. Die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die für die Verwaltungsgerichtsbarkeit zuständigen obersten Landesbehörden übertragen. Die Zulassung der elektronischen Form kann auf einzelne Gerichte oder Verfahren beschränkt werden.

(3) Ein elektronisches Dokument ist eingereicht, sobald die für den Empfang bestimmte Einrichtung des Gerichts es aufgezeichnet hat.

## § 96

(1) Das Gericht erhebt Beweis in der mündlichen Verhandlung. Es kann insbesondere Augenschein einnehmen, Zeugen, Sachverständige und Beteiligte vernehmen und Urkunden heranziehen.

(2) Das Gericht kann in geeigneten Fällen schon vor der mündlichen Verhandlung durch eines seiner Mitglieder als beauftragten Richter Beweis erheben lassen oder durch Bezeichnung der einzelnen Beweisfragen ein anderes Gericht um die Beweisaufnahme ersuchen.

## § 99

(1) Behörden sind zur Vorlage von Urkunden oder Akten und zu Auskünften verpflichtet. Wenn das Bekanntwerden des Inhalts dieser Urkunden oder Akten und dieser Auskünfte dem Wohl des Bundes oder eines deutschen Landes Nachteile bereiten würde oder wenn die Vorgänge nach einem Gesetz oder ihrem Wesen nach geheimgehalten werden müssen, kann die zuständige oberste Aufsichtsbehörde die Vorlage von Urkunden oder Akten und die Erteilung der Auskunft verweigern.

(2) Auf Antrag eines Beteiligten stellt das Oberverwaltungsgericht ohne mündliche Verhandlung durch Beschluss fest, ob die Verweigerung der Vorlage der Urkunden oder Akten oder der Erteilung von Auskünften rechtmäßig ist. Verweigert eine oberste Bundesbehörde die Vorlage oder Auskunft mit der Begründung, das Bekanntwerden des Inhalts der Urkunden, der Akten oder der Auskünfte würde dem Wohl des Bundes Nachteile bereiten, entscheidet das Bundesverwaltungsgericht; Gleiches gilt, wenn das Bundesverwaltungsgericht nach § 50 für die Hauptsache zuständig ist. Der Antrag ist bei dem für die Hauptsache zuständigen Gericht zu stellen. Dieses gibt den Antrag und die Hauptsacheakten an den nach § 189 zuständigen Spruchkörper ab. Die oberste Aufsichtsbehörde hat die nach Absatz 1 Satz 2 verweigerten Urkunden oder Akten auf Aufforderung dieses Spruchkörpers vorzulegen oder die verweigerten Auskünfte zu erteilen. Sie ist zu diesem Verfahren beizuladen. Das Verfahren unterliegt den Vorschriften des materiellen Geheimschutzes. Können diese nicht eingehalten werden oder macht die zuständige Aufsichtsbehörde geltend, dass besondere Gründe der Geheimhaltung oder des Geheimschutzes einer Übergabe der Urkunden oder Akten an das Gericht entgegenstehen, wird die Vorlage nach Satz 5 dadurch bewirkt, dass die Urkunden oder Akten dem Gericht in von der obersten Aufsichtsbehörde bestimmten Räumlichkeiten zur Verfügung gestellt werden. Für

die nach Satz 5 vorgelegten Akten und für die gemäß Satz 8 geltend gemachten besonderen Gründe gilt § 100 nicht. Die Mitglieder des Gerichts sind zur Geheimhaltung verpflichtet; die Entscheidungsgründe dürfen Art und Inhalt der geheim gehaltenen Urkunden oder Akten und Auskünfte nicht erkennen lassen. Für das nichtrichterliche Personal gelten die Regelungen des personellen Geheimschutzes. Soweit nicht das Bundesverwaltungsgericht entschieden hat, kann der Beschluss selbständig mit der Beschwerde angefochten werden. Über die Beschwerde gegen den Beschluss eines Oberverwaltungsgerichts entscheidet das Bundesverwaltungsgericht. Für das Beschwerdeverfahren gelten die Sätze 4 bis 11 sinngemäß.

## **GBO**

### **§ 126**

(1) Die Landesregierungen können durch Rechtsverordnung bestimmen, daß und in welchem Umfang das Grundbuch in maschineller Form als automatisierte Datei geführt wird. Hierbei muß gewährleistet sein, daß

1. die Grundsätze einer ordnungsgemäßen Datenverarbeitung eingehalten, insbesondere Vorkehrungen gegen einen Datenverlust getroffen sowie die erforderlichen Kopien der Datenbestände mindestens tagesaktuell gehalten und die originalen Datenbestände sowie deren Kopien sicher aufbewahrt werden;
2. die vorzunehmenden Eintragungen alsbald in einen Datenspeicher aufgenommen und auf Dauer inhaltlich unverändert in lesbarer Form wiedergegeben werden können;
3. die nach der Anlage zu diesem Gesetz erforderlichen Maßnahmen getroffen werden.

Die Landesregierungen können durch Rechtsverordnung die Ermächtigung nach Satz 1 auf die Landesjustizverwaltungen übertragen.

(2) Die Führung des Grundbuchs in maschineller Form umfaßt auch die Einrichtung und Führung eines Verzeichnisses der Eigentümer und der Grundstücke sowie weitere, für die Führung des Grundbuchs in maschineller Form erforderliche Verzeichnisse. Das Grundbuchamt kann für die Führung des Grundbuchs auch Verzeichnisse der in Satz 1 bezeichneten Art nutzen, die bei den für die Führung des Liegenschaftskatasters zuständigen Stellen eingerichtet sind; diese dürfen die in Satz 1 bezeichneten Verzeichnisse insoweit nutzen, als dies für die Führung des Liegenschaftskatasters erforderlich ist.

(3) Die Datenverarbeitung kann im Auftrag des nach § 1 zuständigen Grundbuchamts auf den Anlagen einer anderen staatlichen Stelle oder auf den Anlagen einer juristischen Person des öffentlichen Rechts vorgenommen werden, wenn die ordnungsgemäße Erledigung der Grundbuchsachen sichergestellt ist.



POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

Oberste Bundesbehörden

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin

POSTANSCHRIFT 11014 Berlin

TEL +49 (0)1888 681-2335

FAX +49 (0)1888 681-2440

BEARBEITET VON A. Schlatmann

E-MAIL V5@bmi.bund.de

INTERNET www.bmi.bund.de

DATUM Berlin, 1. Oktober 2004

AZ V 5a - 130 210/16

BETREFF **Amtliche Beglaubigungen von Dokumenten und Unterschriften (§§ 33, 34 VwVfG)**

BEZUG Mein Rundschreiben vom 8. Dezember 1976 - V II 3 - 130 210/16

## I. Beglaubigung von Schriftstücken

### 1. Allgemein

Nach § 33 Abs. 1 Satz 2 des Verwaltungsverfahrensgesetzes (VwVfG) sind die von der Bundesregierung durch Rechtsverordnung bestimmten Behörden des Bundes und der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie die nach Landesrecht zuständigen Behörden befugt, Abschriften fremder Schriftstücke amtlich zu beglaubigen. Zur Beglaubigung von Abschriften eigener Schriftstücke ist jede Behörde kraft Gesetzes befugt (§ 33 Abs. 1 Satz 1 VwVfG).

Die Bundesregierung hat die Beglaubigungsbefugnis allen Bundesbehörden im Sinne des § 1 Abs. 1 Nr. 1 VwVfG erteilt (Verordnung vom 13. März 2003, BGBl. I S. 361). Die Vorschriften über die Beglaubigung von Abschriften gelten entsprechend für Ablichtungen, Lichtdrucke und ähnliche in technischen Verfahren hergestellte Vervielfältigungen, für auf fototechnischem Wege von Schriftstücken hergestellte Negative, die bei einer Behörde aufbewahrt werden sowie für Ausdrücke elektronischer Dokumente; beglaubigte Vervielfältigungen, Negative und Ausdrücke elektronischer Dokumente stehen beglaubigten Abschriften gleich (§ 33 Abs. 6 VwVfG).

Die Beglaubigung von Abschriften, Vervielfältigungen und Negativen hat zur Voraussetzung, dass die Urschrift von einer Behörde ausgestellt ist oder die Abschrift usw. zur Vorlage bei einer Behörde benötigt wird, sofern nicht durch Rechtsvorschrift die Erteilung beglaubigter



Abschriften aus amtlichen Registern und Archiven, z. B. die Erteilung von Personenstands-  
kunden, anderen Behörden ausschließlich vorbehalten ist.

Abschriften dürfen nicht beglaubigt werden, wenn Umstände zu der Annahme berechtigen,  
dass der ursprüngliche Inhalt des Schriftstückes, dessen Abschrift beglaubigt werden soll,  
geändert worden ist, insbesondere wenn dieses Schriftstück Lücken, Durchstreichungen, Ein-  
schaltungen, Änderungen, unleserliche Wörter, Zahlen oder Zeichen, Spuren der Beseitigung  
von Wörtern, Zahlen oder Zeichen enthält oder wenn der Zusammenhang eines aus mehreren  
Blättern bestehenden Schriftstückes aufgehoben ist (§ 33 Abs. 2 VwVfG).

Nach § 33 Abs. 3 Satz 1 VwVfG wird eine Abschrift beglaubigt durch einen Beglaubigungs-  
vermerk, der unter die Abschrift zu setzen ist. Aus § 33 Abs. 3 Satz 2 VwVfG ergibt sich,  
welchen Inhalt der Vermerk haben muss. Ich empfehle, dem Beglaubigungsvermerk das fol-  
gende Muster zugrunde zu legen:

„Hiermit wird amtlich beglaubigt, dass die vor-/umstehende Abschrift/Ablichtung  
mit der vorgelegten Urschrift/Ausfertigung/beglaubigten/einfachen/Ab-  
schrift/Ablichtung/Ausdruck der/des .....

.....  
(Bezeichnung des Schriftstückes)

übereinstimmt.

Die Beglaubigung wird nur zur Vorlage bei .....

.....  
(Behörde)

erteilt.

Berlin, den .....

Bundesministerium des Innern  
Im Auftrag

(Siegel)

.....  
(Unterschrift)“

Der Hinweis auf den Verwendungszweck entfällt, wenn die Urschrift von einer Behörde aus-  
gestellt ist (§ 33 Abs. 3 Nr. 3 VwVfG).

Besteht die beglaubigte Abschrift oder Ablichtung aus mehreren Blättern, so sind diese so fest  
miteinander zu verbinden, dass ihre Trennung ohne merkbare Beschädigung nicht möglich ist;  
die Verbindungsstellen sind zu siegeln.

§ 33 VwVfG gilt nicht für die Beglaubigung von Abschriften für den internen Bedarf der Be-  
hörde.

## 2. Besonderheiten bei der Beglaubigung von Ausdrucken elektronischer Dokumente

Bei der Beglaubigung des Ausdrucks eines elektronischen Dokuments ist nach § 33 Abs. 4  
Nr. 3 i. V. m. Abs. 3 Satz 2 Nr. 1 VwVfG die genaue Bezeichnung des elektronischen Doku-  
ments anzugeben. Hierzu ist ein kurzer Inhaltshinweis ausreichend, etwa „Ausfuhrgenehmi-  
gung des Bundesausfuhramtes - Az V 55555-6“.



Für die Beglaubigung des Ausdrucks eines elektronischen Dokuments, das nicht mit einer qualifizierten elektronischen Signatur verbunden ist, empfehle ich, dem Beglaubigungsvermerk das folgende Muster zugrunde zu legen:

„Hiermit wird amtlich beglaubigt, dass der vor-/umstehende Ausdruck mit dem elektronischen Dokument der/des .....

.....

....

(Bezeichnung des Dokuments)

übereinstimmt.

Die Beglaubigung wird nur zur Vorlage bei .....

.....

(Behörde)

erteilt.

Berlin, den .....

Bundesministerium des Innern

Im Auftrag

(Siegel)

.....

(Unterschrift)„

Bei der Beglaubigung eines Ausdrucks eines elektronischen Dokuments, das mit einer qualifizierten elektronischen Signatur verbunden ist, muss der Beglaubigungsvermerk nach § 33 Abs. 5 Satz 1 Nr. 1 VwVfG zusätzlich angeben:

- wen die Signaturprüfung als Inhaber der Signatur ausweist,
- welchen Zeitpunkt die Signaturprüfung für die Anbringung der Signatur ausweist und
- welche Zertifikate mit welchen Daten dieser Signatur zugrunde lagen.

Inhaber der Signatur ist der Signaturschlüssel-Inhaber im Sinne des § 7 Abs. 1 Nr. 1 des Signaturgesetzes (SigG). Nach § 2 Nr. 9 SigG ist dies die natürliche Person, die den Signaturschlüssel besitzt und der die zugehörigen Signaturprüfchlüssel durch qualifizierte Zertifikate zugeordnet sind.

Es sind die bei der Signaturprüfung unmittelbar wahrnehmbaren Daten des der Signatur zugrunde liegenden Zertifikats festzustellen:

- die laufende Nummer des Zertifikats (§ 7 Abs. 1 Nr. 4 SigG)
- Beginn und Ende der Gültigkeit des Zertifikats (§ 7 Abs. 1 Nr. 5 SigG)
- Angaben darüber, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art und Umfang beschränkt ist (§ 7 Abs. 1 Nr. 7 SigG), sowie
- Angaben, ob Attribute des Signaturschlüsselinhabers bestehen (§ 7 Abs. 1 Nr. 9 SigG).



SEITE 4 VON 8 Ich empfehle, dem Beglaubigungsvermerk das folgende Muster zugrunde zu legen:

„Hiermit wird amtlich beglaubigt, dass der Ausdruck mit dem elektronischen Do-  
kument der/des .....

.....  
(Bezeichnung des Dokuments)

übereinstimmt.

Bei der Signaturprüfung wurden folgende Feststellungen gemacht:

Inhaber der Signatur ist Frau/Herr .....

Die Signatur wurde am ..... um ..... mit dem Dokument verbunden.

Der Signatur lag das Zertifikat mit der Nummer ..... ,das von ..... bis ..... gül-  
tig ist, zugrunde.

Das Zertifikat enthielt keine/folgende Beschränkungen der Nutzung des Signatur-  
schlüssels .....

Dem Signaturschlüssel-Inhaber waren keine/folgende Attribute zugewiesen

.....  
Die Beglaubigung wird nur zur Vorlage bei .....

.....  
(Behörde)

erteilt.

Berlin, den .....

Bundesministerium des Innern

Im Auftrag

(Siegel)

.....  
(Unterschrift) „

Statt der schriftlichen Niederlegung der bei der Signaturprüfung festgestellten unmittelbar wahrnehmbaren Daten des der Signatur zugrunde liegenden Zertifikats kann auch ein Bildschirm Ausdruck der Signaturprüfung in den Vermerk einbezogen werden.

Besteht der beglaubigte Ausdruck eines elektronischen Dokuments aus mehreren Blättern, so sind diese so fest miteinander zu verbinden, dass ihre Trennung ohne merkbare Beschädigung nicht möglich ist; die Verbindungsstellen sind zu siegeln.

## II. Beglaubigung von elektronischen Dokumenten

Nach § 33 Abs. 4 Nr. 4 VwVfG können auch elektronische Dokumente beglaubigt werden, wenn sie

- zur Abbildung eines Schriftstücks hergestellt wurden oder
- ein anderes technisches Format als das mit einer qualifizierten elektronischen Signatur verbundene Ausgangsdokument erhalten haben.

Beglaubigte elektronische Dokumente nach § 33 Abs. 4 Nr. 4 VwVfG stehen beglaubigten Abschriften gleich (§ 33 Abs. 6 VwVfG).



Auch elektronische Dokumente nach § 33 Abs. 4 Nr. 4 VwVfG dürfen nicht beglaubigt werden, wenn Umstände zu der Annahme berechtigen, dass der ursprüngliche Inhalt des Ausgangsdokuments, dessen Abbild beglaubigt werden soll, geändert worden ist, insbesondere wenn dieses Dokument Lücken, Durchstreichungen, Einschaltungen, Änderungen, unleserliche Wörter, Zahlen oder Zeichen, Spuren der Beseitigung von Wörtern, Zahlen oder Zeichen enthält oder wenn der Zusammenhang eines aus mehreren Seiten bestehenden Dokuments aufgehoben ist (§ 33 Abs. 2 VwVfG).

Elektronische Dokumente, die zur Abbildung eines Schriftstücks hergestellt wurden, werden regelmäßig durch ein Bilddateiprogramm dargestellt werden. Entsprechend den technischen Möglichkeiten des verwendeten Programms ist der Beglaubigungsvermerk nach dem Text des Schriftstücks ein- oder anzufügen. Der Beglaubigungsvermerk muss dabei die nach § 33 Abs. 3 Satz 2 VwVfG erforderlichen Angaben enthalten. Zusätzlich sind der Name des für die Beglaubigung zuständigen Bediensteten und die Bezeichnung der Behörde, die die Beglaubigung vornimmt, in den Vermerk aufzunehmen (§ 33 Abs. 5 Satz 1 Nr. 2 VwVfG). Die nach § 33 Abs. 3 Satz 2 Nr. 4 VwVfG erforderliche Unterschrift des für die Beglaubigung zuständigen Bediensteten und das Dienstsiegel werden durch eine dauerhaft überprüfbare qualifizierte elektronische Signatur ersetzt.

Ich empfehle, dem Beglaubigungsvermerk das folgende Muster zugrunde zu legen:

„Hiermit wird amtlich beglaubigt, dass das vorstehende elektronische Dokument mit der vorgelegten Urschrift/Ausfertigung/beglaubigten/einfachen/Ab-schrift/Ablichtung/Ausdruck der/des .....  
.....  
(Bezeichnung des Schriftstückes)

übereinstimmt.  
Die Beglaubigung wird nur zur Vorlage bei .....  
.....  
(Behörde)

erteilt.

Berlin, den .....

Bundesministerium des Innern  
Im Auftrag

.....  
(Name des Beglaubigenden) “

Der Vermerk ist dem elektronischen Dokument beizufügen und dieses sodann vom Beglaubigen mit seiner dauerhaft überprüfbaren qualifizierten elektronischen Signatur zu versehen.

Elektronische Dokumente, die ein anderes technisches Format als das mit einer qualifizierten elektronischen Signatur verbundene Ausgangsdokument erhalten haben, also umformatiert worden sind, können in gleicher Weise, wie elektronische Dokumente, die zur Abbildung eines Schriftstücks hergestellt wurden, beglaubigt werden. Da nach der Umformatierung die



qualifizierte elektronische Signatur des Ausgangsdokuments nicht mehr prüfbar ist, muss der Beglaubigungsvermerk zusätzlich die Angaben nach § 33 Abs. 5 Satz 1 Nr. 1 VwVfG enthalten (§ 33 Abs. 5 Satz 2 VwVfG).

Ich empfehle, dem Beglaubigungsvermerk das folgende Muster zugrunde zu legen:

„Hiermit wird amtlich beglaubigt, dass das vorstehende elektronische Dokument mit dem elektronischen Dokument der/des .....  
.....  
(Bezeichnung des Dokuments)

übereinstimmt.  
Bei der Signaturprüfung wurden folgende Feststellungen gemacht:  
Inhaber der Signatur ist Frau/Herr .....  
Die Signatur wurde am ..... um ..... mit dem Dokument verbunden.  
Der Signatur lag das Zertifikat mit der Nummer ..... ,das von ..... bis ..... gültig ist, zugrunde.  
Das Zertifikat enthielt keine/folgende Beschränkungen der Nutzung des Signaturschlüssels .....  
Dem Signaturschlüssel-Inhaber waren keine/folgende Attribute zugewiesen  
.....  
Die Beglaubigung wird nur zur Vorlage bei .....  
.....  
(Behörde)

erteilt.

Berlin, den .....

Bundesministerium des Innern  
Im Auftrag

.....  
(Name des Beglaubigenden) „

### III. Beglaubigung von Unterschriften

Nach § 34 Abs. 1 Satz 1 VwVfG sind die von der Bundesregierung durch Rechtsverordnung bestimmten Behörden und die nach Landesrecht zuständigen Behörden befugt, Unterschriften zu beglaubigen, wenn das unterzeichnete Schriftstück zur Vorlage bei einer Behörde oder bei einer sonstigen Stelle, der auf Grund einer Rechtsvorschrift das unterzeichnete Schriftstück vorzulegen ist, benötigt wird. Die Bundesregierung hat die Beglaubigungsbefugnis allen Bundesbehörden im Sinne des § 1 Abs. 1 Nr. 1 VwVfG erteilt (Verordnung vom 13. März 2003, BGBl. I S. 361). Die amtliche Beglaubigung von Unterschriften ohne zugehörigen Text sowie von Unterschriften, die der öffentlichen Beglaubigung (§ 129 des Bürgerlichen Gesetzbuches) bedürfen, ist unzulässig (§ 34 Abs. 1 Satz 2 VwVfG).

Eine Unterschrift soll nur beglaubigt werden, wenn sie in Gegenwart des beglaubigenden Be-  
diensteten vollzogen oder anerkannt wird (§ 34 Abs. 2 VwVfG).



SEITE 7 VON 8

Nach § 34 Abs. 4 VwVfG gelten die Vorschriften über die amtliche Beglaubigung von Unterschriften für die Beglaubigung von Handzeichen entsprechend.

§ 34 Abs. 3 VwVfG schreibt vor, dass der Beglaubigungsvermerk unmittelbar bei der Unterschrift, die beglaubigt werden soll, anzubringen ist, und welchen Inhalt er haben muss. Ich empfehle für den Beglaubigungsvermerk das folgende Muster:

„Die/Das vorstehende Unterschrift/Handzeichen ist von

.....  
(Vorname, Familienname, ggfs. Geburtsname)

wohnhaft in .....  
(Ort, Straße und Hausnummer)

persönlich bekannt – ausgewiesen durch .....  
(Personalausweis, Pass)

vor mir vollzogen – anerkannt – worden.

Dies wird hiermit amtlich beglaubigt.

Die Beglaubigung wird nur zur Vorlage bei .....  
(Behörde oder Stelle)

erteilt.

Berlin, den .....

(Siegel)

Bundesministerium des Innern  
Im Auftrag

.....  
(Unterschrift) „

Besteht das unterzeichnete Schriftstück aus mehreren Blättern, so sind diese so miteinander zu verbinden, dass ihre Trennung ohne merkbare Beschädigung nicht möglich ist; die Verbindungsstellen sind zu siegeln.

§ 34 VwVfG gilt nicht für die Beglaubigung von Unterschriften, die in amtlicher Eigenschaft geleistet werden.

IV.

Ich bitte, in Ihrem Geschäftsbereich nach dem Vorgesagten zu verfahren.



Dieses Schreiben ersetzt mein Rundschreiben vom 8. Dezember 1976 - V II 3 - 130 210/16.

Im Auftrag  
Dr. Schmitz



Beglaubigt.

*Schmitt*  
Angestellte