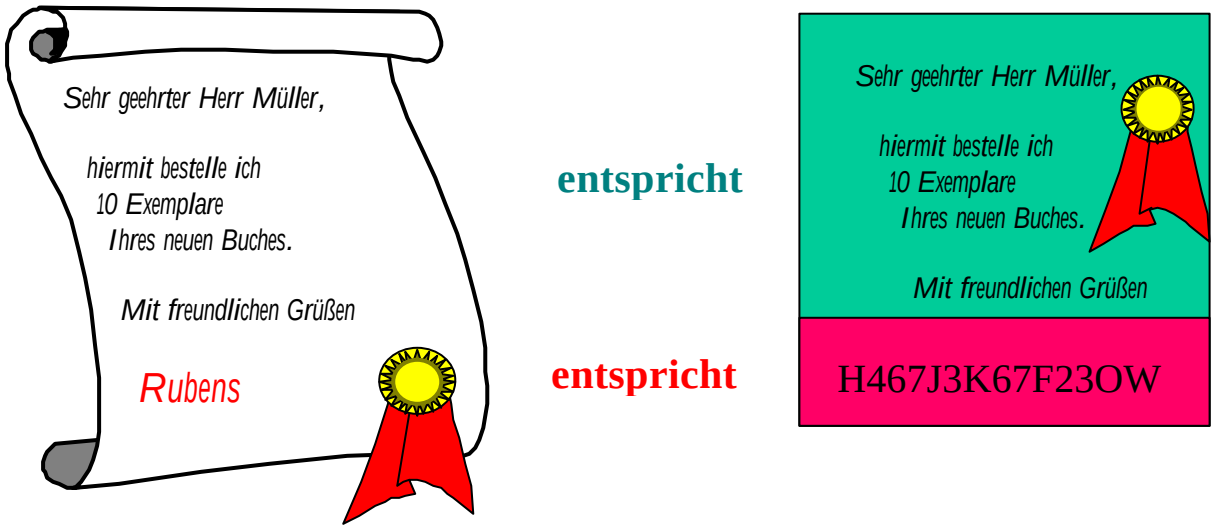
RegTP

Regulierungsbehörde für Telekommunikation und Post

Die digitale Signatur



Herausgeber: Referat IS 15

Inhaltsverzeichnis

I. Die Entwicklung des elektronischen Handels

Die Telematik (*Tele*kommunikation und Infor*matik*) - und damit verbunden der elektronische Handel (electronic commerce) - hat bereits mit ständig steigender Tendenz in allen Lebensbereichen Einzug gehalten, am Arbeitsplatz ebenso wie im privaten Bereich.

Die elektronische Post (z. B. E-Mail) ersetzt dabei schon in vielen Fällen den herkömmlichen Brief in Papierform. Papiergebundene Dokumentation und Kommunikation weichen in zunehmendem Maße neuen elektronischen Medien. Nicht nur wegen des enormen Einsparpotentials und absehbarer Produktionssteigerung wollen Industrie und Nutzer diesen Wandel schnellstmöglich -soweit technologisch realisierbar- vollziehen.

II. Ableitung des Handlungsbedarfs

Elektronische Daten können jedoch nicht wie Papierdokumente in der bisherigen Weise eigenhändig unterschrieben werden. Hier bedarf es eines neuen Mittels: einer elektronischen Unterschrift; eine Form hiervon ist die digitale Signatur.

Praktisch ist die digitale Signatur aber keine eigenhändige Unterschrift, sondern vielmehr eine Art von elektronischem Siegel, mit dem digitale Daten vor Manipulationen geschützt werden.

III. Rechtsgrundlagen

Artikel 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG) vom 22. Juli 1997 enthält das „Gesetz zur digitalen Signatur (Signaturgesetz - SigG)“, welches am 01.08.1997 in Kraft getreten ist.

Basierend auf § 16 SigG ist die Verordnung zur digitalen Signatur (Signaturverordnung - SigV) vom 22. Oktober 1997 am 01.11.1997 in Kraft getreten.

Zweck des Gesetzes ist es, Rahmenbedingungen zu schaffen, unter denen digitale Signaturen als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können.

IV. Beweiskraft digitaler Signaturen

Gesetzlich verankert in den §§ 415 ff Zivilprozeßordnung (ZPO) und in der Rechtsprechung abgesichert gilt seit langer Zeit das mit eigener Hand unterschriebene Schriftstück als Urkunde. Dieses stärkste Beweismittel der ZPO wird definiert als die Verkörperung einer Gedankenäußerung in Schriftzeichen.

Demnach sind Aufzeichnungen auf elektronischen Datenträgern (Textform) schon mangels Schriftform keine Urkunden im Sinne der ZPO, da den Ausdrucken bzw. den Daten die handschriftliche Unterschrift fehlt.

Daraus folgt aber auch, daß bei bestimmten Rechtsvorgängen oder Formvorschriften, in denen die Schriftform (mit eigenhändiger Unterschrift) oder notarielle Beglaubigung vorgeschrieben werden, derzeit keine digitalen Signaturen[1] zugelassen sind. Die Bun-

[1] Mit „digitalen Signaturen“ in diesem Beitrag sind grundsätzlich solche im Sinne des § 1 Abs. 1 SigG gemeint.

desregierung - unter Federführung des Justizministeriums - bereitet jedoch eine Reform dieser Vorschriften vor, die zum Ziel hat, daß in den Bereichen, in denen die Schriftform weiterhin verlangt wird, die digitale Signatur daneben zugelassen und um entsprechende Beweisregelungen hierzu ergänzt wird. Denn:

Wenn ein elektronisches Dokument mit digitaler Signatur nach dem Signaturgesetz nachweislich eine weitaus höhere Sicherheit vor Verfälschung als ein herkömmliches Schriftdokument mit eigenhändiger Unterschrift bietet, darf ein solches Dokument folglich beweisrechtlich nicht schlechter gestellt werden.

Allerdings ist für die meisten Rechtsgeschäfte vom Gesetzgeber keine bestimmte Form vorgeschrieben und die Partner können sich frei vereinbaren, sogar per Handschlag oder auch per Fax oder E-Mail. Juristisch spricht man hier vom „formfreien Bereich". Wer aber sicher gehen will, verwendet bei wichtigen oder besonders risikobehafteten Rechtsgeschäften seit jeher die Schriftform oder bei digitalen Daten zukünftig die digitale Signatur, um im Falle einer gerichtlichen Auseinandersetzung eine entsprechende Beweisführung erbringen zu können.

A. Beweiskraft von digitalen Dokumenten und schriftlichen Dokumenten (mit eigenhändiger Unterschrift) im Vergleich

Elektronische Daten können durch technische oder menschliche Fehler oder auch gezielte Manipulation beliebig und ohne Spuren verändert werden. Auch ist u. U. der Urheber eines digitalen Dokumentes nicht mehr festzustellen. So ist es leicht möglich, das Abbild einer eigenhändigen Unterschrift in elektronische Daten einzufügen, beispielsweise durch einscannen; und dann problemlos - auch von Unbefugten - beliebig oft zu kopieren und unter beliebige Daten zu setzen.

Es bleibt also immer die Frage offen, ob das vorliegende Dokument mit diesem Inhalt tatsächlich von einer bestimmten Person stammt; daher haben derartige digitale Dokumente grundsätzlich keine Beweiskraft.

In diesem Zusammenhang darf jedoch folgendes nicht vergessen werden:

Auch herkömmliche, papierene Unterlagen können manipuliert werden. Insbesondere durch den Einsatz moderner Technologien - z. B. Schreibautomaten - sind mittlerweile aber auch eigenhändige Unterschriften relativ leicht, aber schwer nachweisbar, zu fälschen. Auch Inhalte eines Schriftdokumentes können unter Umständen unbemerkt verändert werden, bspw. durch Streichung von Textpassagen oder Hinzufügen von Zahlen. So läßt es sich im Nachhinein dann nicht immer beweisen, ob die Änderungen nach oder vor der Unterschrift erfolgt sind.[2]

Jetzt bietet die gesetzlich anerkannte digitale Signatur für elektronische Dokumente eine weitaus höhere Fälschungssicherheit, als sie bei papiergebundenen, schriftlichen Urkunden gegeben ist. Anhand einer solchen digitalen Signatur kann zuverlässig festgestellt werden, daß Daten

- von einer bestimmten Person signiert wurden (*Urheberschaft, Non-Repudiation*) und
- nach erfolgter Signatur in keiner Weise (einschließlich Punkt und Komma oder speziellen Formatierungen) verändert wurden (*Integrität und Authentizität*).

[2] Vgl. zu diesem Themenkomplex: Bieser, Kersten „Chipkarte statt Füllfederhalter", Hüthig - Verlag 1998.

Die digitale Signatur schützt dabei nicht - genau wie die eigenhändige Unterschrift - die Vertraulichkeit des Inhaltes. Die Daten sind durch sie nicht vor unbefugter oder unerwünschter Kenntnisnahme Dritter geschützt. Ein derartiger Schutz kann nur durch eine geeignete Verschlüsselung erreicht werden - gegebenenfalls zusätzlich zu der digitalen Signatur. Dies fällt aber nicht unter den Regelungsbereich des Signaturgesetzes und ist daher strikt von der digitalen Signatur zu trennen - auch wenn das Verfahren der digitalen Signatur auf den gleichen mathematischen bzw. technischen Grundlagen basiert.

B. Realisierung der hohen Fälschungssicherheit in der Praxis

Der Anspruch der hohen Fälschungssicherheit, den § 1 Abs.1 SigG stellt, wird insbesondere durch das Zusammenwirken der folgenden Punkte realisiert:

1.) An das Personal der Zertifizierungsstelle[3] werden hohe Anforderungen in punkto Zuverlässigkeit und Fachkompetenz gestellt.

2.) Durch infrastrukturelle Sicherungsmaßnahmen werden sicherheitsrelevante Bereiche vor unbefugtem Zutritt und sicherheitsrelevante technische Komponenten vor unberechtigtem Zugriff geschützt.

3.) In der Aufbauorganisation wird z. B. durch Rollentrennung sichergestellt, daß dieselbe Person nicht gleichzeitig mehrere bestimmte Tätigkeiten wahrnimmt (sogenannte Unvereinbarkeiten).

4.) In der Ablauforganisation sind Schutzprinzipien wie z. B. das Vier-Augen-Prinzip bei der Ausführung bestimmter Tätigkeiten sicherzustellen.

5.) Technische Sicherheit wird erreicht durch:

- nicht zu brechende mathematischen Verfahren,
- einmalige Signaturschlüssel und absolute Geheimhaltung des privaten Signaturschlüssels,
- zuverlässige Bindung des privaten Signaturschlüssels an den rechtmäßigen Inhaber,
- den Ausschluß nicht gewollter digitaler Signaturen,
- die zuverlässige Prüfung digitaler Signaturen, sowie
- den Einsatz von technischen Komponenten, die hinsichtlich der Erfüllung der besonderen Sicherheitsanforderungen geprüft und bestätigt sind, in Verbindung mit einer definierten Anwender- bzw. Einsatzumgebung.

6.) Schließlich finden Kontrollen und Prüfungen der Zertifizierungsstellen statt, um festzustellen, ob - auch im laufenden Betrieb - die Anforderungen aus dem Signaturgesetz und der Signaturverordnung eingehalten worden sind bzw. werden. Festgestellte Verstöße gegen Gesetz und Verordnung können dabei auch sanktioniert werden.

7.) Zuletzt hat eine umfassende Unterrichtung der Signaturschlüssel-Inhaber über die Maßnahmen zu erfolgen, welche die sichere Anwendung und die Sicherheit einer digitalen Signatur gewährleisten.

V. Funktionsweise der digitalen Signatur

Der Anwender einer digitalen Signatur ist von der komplexen Realisierung der Fälschungssicherheit kaum betroffen: er muß vor allem sicherstellen, daß sein privater Sig-

[3] Begriff und Funktion einer Zertifizierungsstelle siehe unten Kapitel V C. und VI.

naturschlüssel nicht unberechtigt benutzt werden kann. Die Kenntnisse von der Funktionsweise der digitalen Signatur können sich dabei in Grenzen halten, da es keiner aufwendigen Mittel und Vorgehensweisen bedarf, um eine digitale Signatur in Praxi zu erzeugen oder zu prüfen.

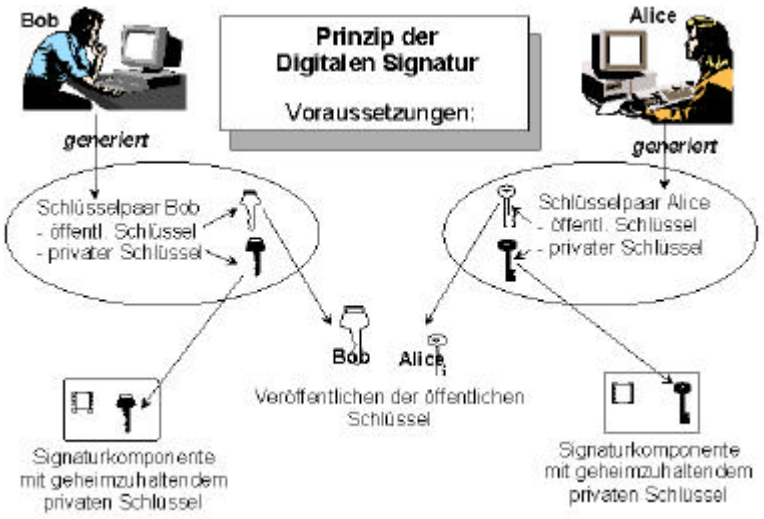
Will man mehr als ein unwissender Anwender sein, kann aber das Grundprinzip der digitalen Signatur mittels der vereinfachten, nachfolgenden Beschreibung vor Augen geführt werden.

A. Asymmetrisches Verfahren

Wie bereits erwähnt, beruht das Prinzip der digitalen Signatur auf einem mathematischen, kryptographischen Verfahren, dem asymmetrischen Verschlüsselungsverfahren.

Asymmetrisches Verfahren bedeutet, daß bei der Signaturbildung ein anderer Schlüssel eingesetzt wird als bei der Signaturprüfung: Jeder Benutzer erhält zwei verschiedene, komplementäre Schlüssel (Schlüsselpaar), einen geheimen, privaten (*private key*) und einen öffentlichen Schlüssel (*public key*). Der öffentliche Schlüssel wird - wie aus dem Namen schon ersichtlich - öffentlich bekannt gegeben, er ist allgemein zugänglich. Der andere, private Schlüssel ist geheim zu halten und dies bedeutet absolute Geheimhaltung[4].

Wichtige Bedingungen für die Sicherheit der digitalen Signatur sind in diesem Zusammenhang, daß die für die Schlüsselgenerierung verwendeten Algorithmen, sowie die dazugehörigen Parameter „sicher“[5] sind, daß das jeweilige Schlüsselpaar einmalig ist und daß aus dem öffentlichen Schlüssel nicht der private Schlüssel errechnet werden kann.



[4] Sowohl bei der Schlüsselerzeugung als auch Speicherung auf der Signaturkomponente darf niemand, auch nicht der Signaturschlüssel-Inhaber selbst, Kenntnis vom privaten Schlüssel erhalten. Dies schließt auch eine Speicherung außerhalb der Signaturkomponente aus (sog. „Schlüsselhinterlegung“ oder key escrow/key recovery).

[5] Sicher im Sinne von „nicht-zu-brechen“ nach dem derzeitigen Stand der Technik.

B. Verwendung der Schlüssel

Mit dem geheimen, **privaten** Schlüssel, der sich **nur** auf einer Signaturkomponente befindet (in der Regel auf einer nicht auslesbaren[6], besonderen Chipkarte), wird die digitale Signatur durch den rechtmäßigen Besitzer erzeugt, während mit dem dazugehörigen **öffentlichen** Schlüssel die digitale Signatur vom Empfänger überprüft werden kann[7].

1. Signaturbildung (privater Schlüssel)

Zur Erzeugung digitaler Signaturen wird als weiterer kryptographischer Mechanismus eine sogenannte Hash-Funktion benötigt. Diese wird vor der Signatur dazu benutzt, die zu signierende Nachricht auf den Hashwert[8] zu reduzieren (komprimieren). Signiert wird dann nicht die Nachricht selbst, sondern ihr Hashwert; das Ergebnis stellt die digitale Signatur dar. Diese wird automatisch an das Originaldokument angehängt und anschließend mit dem Originaldokument elektronisch an den Empfänger übermittelt. Auf diese Weise spart man Rechenzeit, Speicherplatz und Übertragungszeit.

Anzumerken ist hier, daß die Sicherheit der digitalen Signatur gegen Fälschungen und Verfälschungen an dieser Stelle auch von der kryptographischen Stärke der Hashfunktion abhängt. Hashwerte müssen „kollisionsfrei“ und die Hashfunktion eine „Einwegfunktion“ sein.

Wenn Kollisionen - d. h. unterschiedliche Nachrichten mit demselben Hashwert - auftreten würden, kann die Ersetzung der eigentlichen Nachricht durch ihren Hashwert nämlich beim Signieren zu Sicherheitsproblemen führen: Wird eine dieser Nachrichten signiert, so kann der „Verifizieralgorithmus“ des öffentlichen Schlüssels nicht erkennen, ob die Nachricht gegen eine solche andere ausgetauscht wurde. Die Bindung zwischen einer Nachricht und ihrem Hashwert muß demnach unauflösbar, eindeutig bzw. einzigartig sein.

Mit anderen Worten: Eine Hashfunktion muß praktisch kollisionsresistent[9] sein; wenn diese Eigenschaft verletzt wäre, könnte man signierte Dokumente fälschen.

Eine Hashfunktion muß zudem eine Einwegfunktion sein, d. h. es ist unmöglich, zu einem vorgegebenen Hashwert eine dazugehörige Nachricht zu finden. Andernfalls könnte man auch dann signierte Dokumente fälschen.

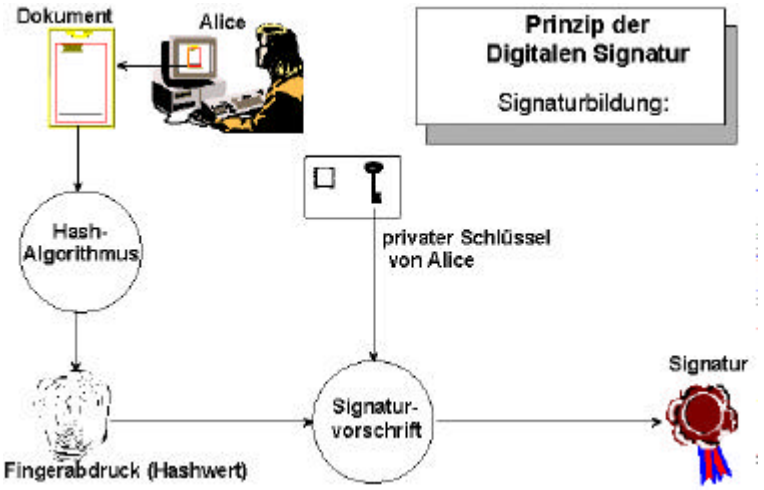
---

[6] Das Auslesen des geheimen Schlüssels oder der Authentisierungsdaten (s. u.) würde den Mißbrauch des Signaturschlüssels ermöglichen.

[7] Der öffentliche Schlüssel wird deshalb auch „Prüfschlüssel“ oder „Verifizierschlüssel“ genannt. Dieser kann z. B. der Nachricht vor der Absendung „angehängt“ werden.

[8] „Hash“ ist der englische Begriff für „Zerhacktes“

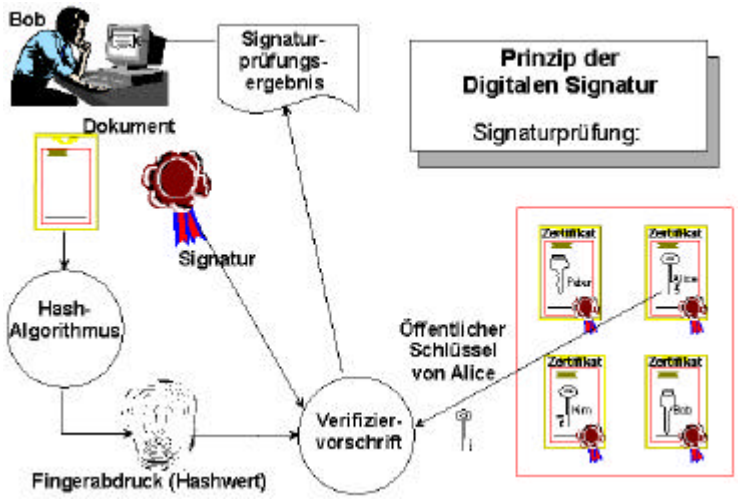
[9] Die Kollisionsresistenz besagt, daß eine ein-eindeutige Beziehung zwischen einer Nachricht und ihrem Hashwert gegeben ist. Deswegen nennt man den Hashwert einer Nachricht anschaulich auch einen digitalen Fingerabdruck.



2. Signaturprüfung (Öffentlicher Schlüssel)

Die Prüfung beim Empfänger der Nachricht erfolgt in umgekehrter Reihenfolge: Der signierte Hashwert wird mit dem angehängten öffentlichen Schlüssel des Absenders „entschlüsselt“ (dechiffriert). Das Resultat ist der Hashwert der Originalmeldung bzw. des Originaldokumentes. Gleichzeitig wird vom Empfänger mit der Hashfunktion auch der Hashwert des mitgeschickten Dokuments, auf den sich die digitale Signatur beziehen soll, berechnet. Gelingt dies, wird der zweite Hashwert nun mit dem aus der Signatur dechiffrierten Hashwert verglichen: Stimmen die Resultate überein, ist die digitale Signatur authentisch.

Wenn nun aber die Originalmeldung während der Übermittlung verändert wird[10] (ein Bit genügt!), so wird sich auch deren Hashwert ändern. Somit würde der Empfänger feststellen, daß der Hashwert, den er aufgrund der Originalmeldung berechnet hat, nicht mit dem aus der Signatur dechiffrierten Hashwert übereinstimmt. Als Konsequenz wird er das Dokument nicht akzeptieren, da entweder das signierte Dokument verfälscht oder die digitale Signatur gefälscht wurde.



[10] Dies kann durch nie ganz auszuschließende technisch bedingte Verfälschungen oder aufgrund gezielter Manipulationen der Fall sein.

Folglich hat der Empfänger bei einer erfolgreichen Überprüfung der digitalen Signatur die Garantie, daß die Meldung nicht verändert wurde (*Integrität*).

Es bleibt bis hierher allerdings die Frage offen, wie man erkennen kann, daß die Signatur eines Dokumentes einer bestimmten Person zuzuordnen ist (*Urheberschaft*).

C. Zertifizierung des öffentlichen Schlüssels (Signaturschlüssel-Zertifikat)

Da nur der berechtigte Besitzer in der Lage ist, durch eine entsprechende *Authentisierung* den privaten Signaturschlüssel anzuwenden, kann nur er die digitale Signatur erstellen[11]. Somit müßte der Empfänger eines digital signierten Dokuments eigentlich nachweisen können, daß die Signatur nur dieser bestimmten Person zuzuordnen ist (Nichtabstreitbarkeit der Urheberschaft oder *Non-Repudiation*).

Nun bleibt aber hier noch ein (weiteres) Sicherheitsproblem, nämlich die Echtheitsgarantie des öffentlichen Schlüssels des Absenders, denn:

Der Empfänger einer digital signierten Nachricht hat bis jetzt keine Garantie, daß der öffentliche Schlüssel[12] tatsächlich vom Absender stammt.

Die Signatur selbst kann zwar gültig sein, der damit verbundene öffentliche Schlüssel kann aber theoretisch von einem Betrüger oder einer „erfundenen“ (fiktiven) Person stammen.

Nehmen wir also an, daß ein Krimineller bei einem Händler eine teure Ware bestellen will. Hierzu generiert er sich selbst sein Schlüsselpaar, signiert mit seinem privaten Signaturschlüssel und verschickt die Bestellung zusammen mit seinem angehängten öffentlichen Schlüssel an den Empfänger (Händler), und zwar unter einem falschen Namen.

Der Händler kann zwar noch feststellen, daß die Signatur korrekt ist, aber nicht, ob die Bestellung von der Person stammt, für die sie sich ausgibt oder ob die Person wirklich existiert.

Folglich braucht der Empfänger einer solchen Meldung Gewißheit darüber, daß der öffentliche Schlüssel tatsächlich einer bestimmten Person zuzuordnen ist.

Eine Möglichkeit bestünde bspw. darin, daß zwei Geschäftspartner sich persönlich kennen und sich ihre öffentlichen Schlüssel gegenseitig übergeben (bekanntgegeben) haben.

Diese Methode setzt aber voraus, daß sich zwei Personen kennen oder schon einmal vorher getroffen haben, was aber in der Praxis nicht oft der Fall sein wird.

---

[11] Um eine unberechtigte Nutzung des privaten Schlüssels zu verhindern, muß sich der berechtigte Nutzer als solcher ausweisen. Die Authentisierung, d. h. der Nachweis der Benutzungsberechtigung, erfolgt durch Besitz und Wissen (mind. 6-stellige PIN oder anderen geeigneten Code und evtl. zusätzlich biometrische Merkmale, wie z. B. Fingerabdruck). Erst nach erfolgreicher Authentisierung ist die Benutzung des privaten Schlüssels und damit eine digitale Signatur möglich.

[12] und damit auch die digitale Signatur, die - wie erläutert - mit dem dazugehörigen, komplementären privaten Schlüssel erzeugt wird.

Besser ist es, wenn es eine Instanz gäbe, welche die Zuordnung eines öffentlichen Schlüssels[13] zu einer gewissen Person vornimmt, bescheinigt und garantiert. Diese Instanz wird nach dem Signaturgesetz als *Zertifizierungsstelle* (*Certification Authority, CA*) - kurz *ZS* - bezeichnet[14].

Diese stellt ein sogenanntes *Signaturschlüssel-Zertifikat* aus. Gem. § 2 Abs. 3 SigG ist ein solches Zertifikat „ .... eine mit einer digitalen Signatur versehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person ...“. Man kann auch sagen, daß die Zertifizierungsstelle „digitale Identität“ ausstellt. Dies setzt zwangsläufig voraus, daß die ZS die Antragsteller eindeutig und sicher identifiziert, z. B. über einen gültigen Personalausweis.

Damit nun aber eine digitale Signatur auf ihre Urheberschaft überprüft werden kann, muß die Zertifizierungsstelle alle von ihr ausgestellten Zertifikate in einem über die öffentlichen Netze zugänglichen Verzeichnis nachprüfbar halten. Die Nachprüfung muß „... jederzeit für jeden ...“ ermöglicht werden[15].

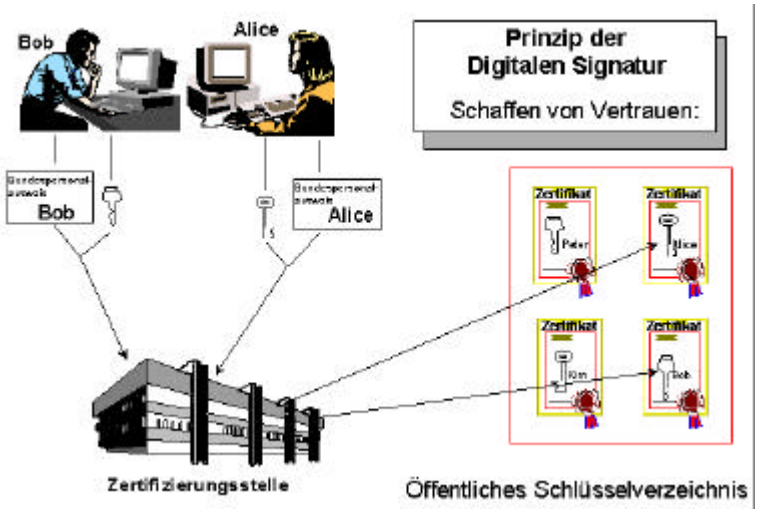
Selbst wenn nun ein Nachprüfender eine entsprechende Abfrage vornimmt: Wie kann er sicher sein, daß Daten für Zertifikate authentisch und unverfälscht sind? Nun, die Zertifizierungsstelle garantiert mit ihrer digitalen Signatur unter den Zertifikatsdaten der Signaturschlüssel-Inhaber hierfür[16].

Um dies sicherzustellen, hat die Zertifizierungsstelle

- Vorkehrungen zu treffen, damit Daten für Zertifikate nicht unbemerkt[17] gefälscht oder verfälscht werden können,
- Maßnahmen zu ergreifen, die die privaten Signaturschlüssel und eingesetzten technischen Komponenten vor unbefugtem Zugriff schützen, und
- technische Komponenten mit Sicherheitsvorkehrungen einzusetzen, die Fälschungen digitaler Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung privater Signaturschlüssel schützen.[18]

Man kann also sagen, daß eine Zertifizierungsstelle eine Garantenfunktion für authentische Signaturschlüssel-Zertifikate sowie deren Integrität übernimmt.

[13] Damit bürgt sie gleichzeitig dafür, daß auch der dazugehörige private Schlüssel der Person gehört.
[14] Diese *Zertifizierungsstelle* i. S. des SigG ist nicht mit einer nach DIN EN 45011 akkreditierten Zertifizierungsstelle zu verwechseln.
[15] Aus dieser Formulierung aus § 5 Abs. 1 SigG lassen sich sehr hohe Verfügbarkeitsanforderungen an den Verzeichnisdienst ableiten, so daß die ZS entsprechende Maßnahmen gegen Brand, Sabotage, Wassereinbruch, Ausfall von Strom oder Telekommunikationsverbindungen usw. treffen muß.
[16] Eine Verfälschung würde bei der Überprüfung der Zertifikat-Signatur zwangsläufig bemerkt werden.
[17] Das bedeutet nicht, daß eine bemerkte (Ver-) Fälschung erlaubt wäre.
[18] S. hierzu www.regtp.de, Button „Digitale Signatur“, *Maßnahmenkataloge*.



Aber: „Sed quis custodiet ipsos custodes (Wer aber bewacht jene Wachen)“[19]?

Oder, bezogen auf die digitale Signatur:

- Wer kontrolliert die Zertifizierungsstellen?
- Wer stellt deren Signaturschlüssel-Zertifikate aus?

VI. Die Sicherungsinfrastruktur

Bei einer unüberschaubaren Anzahl von einander unbekannten Personen, die asymmetrische Kryptoverfahren für die digitale Signatur einsetzen, wird eine vertrauenswürdige Instanz[20] benötigt, die die Identität der jeweiligen Kommunikationspartner garantiert.

Diese Instanz wird im Signaturgesetz (SigG) als Zertifizierungsstelle (ZS) bezeichnet und übernimmt mit ihrer eigenen digitalen Signatur unter den Schlüsselzertifikaten der Teilnehmer eine Garantenfunktion für deren Authentizität und Integrität.

Um also den öffentlichen Schlüssel bzw. das Zertifikat des Absenders einer Nachricht entsprechend überprüfen zu können, benötigt der Empfänger den öffentlichen Schlüssel der ZS.

Hier entsteht ein weiteres Sicherheitsproblem: die ZS verfügt über die Möglichkeit, ihre selbst produzierten Schlüssel selbst zu zertifizieren. Theoretisch würde das einem Kriminellen die Möglichkeit eröffnen, sich als ZS zu betätigen, und mit selbst ausgestellten ZS-Zertifikaten falsche Schlüsselzertifikate zu produzieren und zu verteilen.

Um dies zu vermeiden und um sicherzustellen, daß Zertifizierungsstellen die hohen Sicherheitsanforderungen des SigG erfüllen und damit die (Rechts-)Sicherheit der digitalen Signatur gewährleisten, sowie die weiteren, wichtigen Funktionen einer Sicherungsinfrastruktur erfüllen, sieht das Signaturgesetz zusätzlich eine unabhängige Instanz vor, die hierfür mit entsprechenden Befugnissen versehen worden ist.

---

[19] Zitat von Juvenal

[20] Im Zusammenhang mit der gesetzeskonformen digitalen Signatur sollte bei dem oft synonym benutzte Ausdruck „vertrauenswürdiger Dritter“ (*„Trusted Third Party -TTP“)* bedacht werden, daß dieser Begriff auch im Kontext mit „Verschlüsselung“ bzw. „Schlüsselhinterlegung (Key Escrow/Recovery)“ verwendet wird. Eine saubere Abgrenzung hierzu ist jedoch von Vorteil.

VII. Die Regulierungsbehörde für Telekommunikation und Post (Reg TP) als zuständige Behörde gem. § 3 SigG[21]

§ 3 Signaturgesetz begründet die Zuständigkeit der Reg TP für
- die Erteilung von Genehmigungen,
- die Ausstellung von Zertifikaten, die zum Signieren von Zertifikaten eingesetzt werden, sowie
- die Überwachung der Einhaltung von SigG und SigV.

A. Genehmigung der Zertifizierungsstellen

Der erste Zuständigkeitsbereich betrifft die Durchführung des Genehmigungsverfahrens und die Entscheidung über die Erteilung einer Genehmigung zum Betrieb einer gesetzeskonformen Zertifizierungsstelle.

Zur Sicherstellung der Vertrauenswürdigkeit sind im Rahmen dieses Genehmigungsverfahrens verschiedene Unterlagen zu prüfen:

1.) Personal: Auf Verlangen ist vom Antragsteller der Nachweis zu erbringen, daß die für den Betrieb einer Zertifizierungsstelle erforderliche Zuverlässigkeit der gesetzlichen Vertreter der ZS gegeben ist.

§ 1 Abs. 2 SigV konkretisiert dies dahingehend, daß der Antragsteller hierfür insbesondere einen aktuellen Handelsregisterauszug, sowie aktuelle Führungszeugnisse nach § 30 Abs. 5 des Bundeszentralregistergesetzes für die gesetzlichen Vertreter der ZS vorlegt.

Zur Feststellung der erforderlichen Fachkunde hat der Antragsteller darzulegen, daß das am Zertifizierungsverfahren oder an der Vergabe von Zeitstempeln[22] beteiligte Personal über die erforderlichen Qualifikationen verfügt. Diese erstrecken sich auf den juristischen sowie den technisch-administrativen Bereich.

2.) Technische Komponenten: Die eingesetzten technischen Komponenten müssen nach dem Stand der Technik hinreichend geprüft und die Erfüllung der Anforderungen aus SigG und SigV durch eine von der Regulierungsbehörde anerkannten Stelle[23] bestätigt sein

3.) Sicherheitskonzept: Die Maßnahmen zur Erfüllung der Sicherheitsanforderungen sind in einem Sicherheitskonzept aufzuzeigen. Dessen Umsetzung muß gleichfalls durch eine anerkannten Stelle geprüft und bestätigt worden sein.

B. Ausstellung von Signaturschlüssel-Zertifikaten

Als weitere Aufgabe überträgt die Vorschrift des § 4 Abs. 5 SigG der Reg TP die Ausstellung von Zertifikaten für Signaturschlüssel von Zertifizierungsstellen, die ausschließlich zum Signieren von Schlüsselzertifikaten einzusetzen sind.

---

[21] Vgl. zu diesem Themenkomplex auch: Roßnagel, MMR 1998, S. 468 ff.

[22] Ein Zeitstempel ist eine mit einer digitalen Signatur versehene digitale Bescheinigung einer ZS, daß ihr bestimmte Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Dies kann dann geboten sein, wenn ein Zeitpunkt im Streitfalle beweiserheblich sein kann. Hierfür muß somit die gleiche Sicherheit wie für das Ausstellen von Zertifikaten gewährleistet sein! Gem. § 9 SigG handelt es sich um eine weitere *Pflichtdienstleistung* einer ZS.

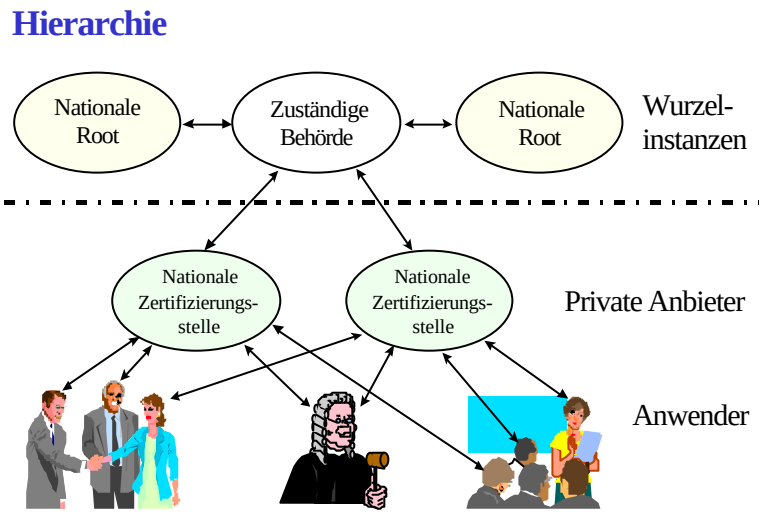
[23] S. nachstehendes Thema „Weitere staatliche Aufgaben“

Hieraus ergibt sich folgende Zertifikatshierarchie:

1. Die zuständige Behörde stellt als oberste Zertifizierungssinstanz das Zertifikat für ihren eigenen öffentlichen Schlüssel selbst aus: das Wurzelzertifikat.[24].
2. Die zuständige Behörde stellt weiterhin die Zertifikate für die öffentlichen Schlüssel der Zertifizierungsstellen aus: Zertifizierungsstellen-Zertifikate.
3. Die jeweilige Zertifizierungsstelle stellt die Zertifikate für die öffentlichen Schlüssel ihrer Kunden aus: Teilnehmerzertifikate.

Der Nachweis, daß es sich um eine gesetzeskonforme Zertifizierungsstelle handelt, ergibt sich im Zweifelsfall also daraus, daß sie für ihren öffentlichen Schlüssel ein Zertifikat der zuständigen Behörde besitzt[25].

Nach § 8 Abs. 2 SigV obliegt darüber hinaus die Anerkennung der Signaturschlüssel-Zertifikate oberster ausländischer Zertifizierungsstellen mittels digitaler Signatur der Reg TP, wobei die Anerkennung nur erfolgt, wenn die betroffenen ausländischen Zertifikate eine gleichwertige Sicherheit aufweisen.



C. Überwachung der Einhaltung von SigG und SigV

Eine weitere Aufgabe, die der Regulierungsbehörde obliegt, ist die Überwachung der Einhaltung der maßgeblichen Rechtsvorschriften:

Sollte eine Person, die öffentliche Signaturschlüssel zertifiziert, fälschlicherweise den Anschein erwecken, eine Genehmigung nach § 4 SigG zu besitzen, kann die Zertifizierungstätigkeit untersagt werden. Für diesen Fall sind umfangreiche Kontrollbefugnisse vorgesehen.

Im Rahmen dieser Überwachungspflichten besteht weiterhin die Aufgabe, die genehmigten Zertifizierungsstellen zu kontrollieren und im Bedarfsfalle Maßnahmen zu ergreifen:

[24] Die zuständige Behörde wird deshalb auch als Wurzelinstanz oder Root bezeichnet.
[25] Dieses kann in dem über öffentliche Telekommunikationsverbindungen erreichbaren Verzeichnisdienst der Reg TP als zuständige Behörde überprüft werden.

So kann die Reg TP, um die Einhaltung von SigG und SigV sicherzustellen, gegenüber einer Zertifizierungsstelle alle geeigneten, erforderlichen und verhältnismäßigen Anordnungen treffen, bspw. die Untersagung der Benutzung ungeeigneter technischer Komponenten. Als Ultima Ratio kann dabei der Betrieb der Zertifizierungsstelle teilweise oder gänzlich untersagt und eine erteilte Genehmigung widerrufen werden.

Die Zertifizierungsstellen haben außerdem im Abstand von zwei Jahren sowie nach jeder sicherheitserheblichen Veränderung eine regelmäßige Prüfung auf ihre Normenkonformität von einer privaten, anerkannten Prüf- und Bestätigungsstelle durchführen zu lassen und der Reg TP den Prüfbericht und die Bestätigung hierüber vorzulegen.[26]

Als Überwachungsaufgaben sind weiterhin die Aufgaben anzusehen, die § 11 SigG der Regulierungsbehörde im Rahmen der Einstellung der Tätigkeiten einer Zertifizierungsstelle überträgt[27], sowie die Überwachungspflichten bzgl. der Prüfung und Bestätigung der Eignung von technischen Komponenten nach § 17 Abs. 3, Sätze 3 bis 5, § 17 Abs. 4 SigV.

Eine Eingriffsermächtigung besteht, wenn die eingesetzten technischen Komponenten Sicherheitsmängel aufweisen, die eine unbemerkte Fälschung digitaler Signaturen oder eine unbemerkte Verfälschung signierter Daten zulassen würden. Gem. § 17 Abs. 3 S. 5 SigV können die hierfür erteilten Bestätigungen für ungültig erklärt werden.

Nach § 13 Abs. 5 SigG hat die Reg TP den elektronischen Rechtsverkehr dahingehend zu beobachten, ob bei ausgestellten Zertifikaten Tatsachen die Annahme rechtfertigen, daß diese gefälscht oder nicht hinreichend fälschungssicher sind oder eingesetzte technische Komponenten Sicherheitsmängel aufweisen. Ggf. ist eine Sperrung dieser Zertifikate anzuordnen.

D. Weitere staatliche Aufgaben[28]

Weitere Verwaltungsaufgaben betreffen: die Anerkennung von privaten Prüf- und Bestätigungsstellen, das Erstellen von Katalogen und Listen sowie Publikationen.

Die Zuständigkeit der Reg TP ergibt sich insoweit kraft Sachzusammenhang, da sie sachlich geeignet ist, die von keiner anderen Stelle erfaßten administrativen Aufgaben zu erfüllen.[29]

1. Anerkennung von Prüf- und Bestätigungsstellen

Weiterhin werden von der Reg TP in ihrer Tätigkeit als zuständige Behörde nach dem Signaturgesetz Prüf- und Bestätigungsstellen anerkannt.

Diese Stellen sind zum einen zur Kontrolle der Zertifizierungsstellen hinsichtlich der Erfüllung der Anforderungen aus SigG und SigV vorgesehen (§ 4 Abs. 3 S. 3 SigG). Zum anderen bestätigen derart anerkannte Stellen die Eignung technischer Komponenten im Sinne des Signaturgesetzes und der Signaturverordnung (§ 14 Abs. 4 SigG). Als „Ver-

[26] vgl. hierzu § 13 SigG und § 15 SigV.
[27] Z. B. Aufsicht darüber, ob die Zertifizierungssstelle, die den Betrieb einstellt, für eine Übernahme der Tätigkeit durch eine andere ZS sorgt und diese ordnungsgemäß erfolgt, und ob sie den Informationspflichten gegenüber ihren Signaturschlüssel-Inhabern nachkommt - vgl. § 11 SigG und § 14 SigV.
[28] vgl. hierzu *Roßnagel*, MMR 1998, S. 468 ff (471ff).
[29] vgl. Roßnagel, MMR 1998, S. 468 ff (S. 472).

waltungshelfer“[30] werden diese Stellen mit eigenen Entscheidungsbefugnissen tätig und unterstützen die Regulierungsbehörde.

2. Erstellen von Katalogen und Listen

Zur konstruktiven Unterstützung von Herstellern von technischen Komponenten, den Betreibern von ZS sowie den Nutzern führt die Reg TP unter anderem jeweils einen Katalog

- von geeigneten Sicherheitsmaßnahmen zur Erstellung eines Sicherheitskonzeptes gem. § 12 Abs. 2 SigV, sowie
- von geeigneten Sicherheitsmaßnahmen für technische Komponenten gem. § 16 Abs. 6 SigV.

3. Publikationen

Damit diese und andere relevante Informationen auch den Adressaten zur Verfügung stehen, sind diese im Bundesanzeiger zu veröffentlichen. Die bestätigten technischen Komponenten, sowie die anerkannten Prüf- und Bestätigungsstellen sind außerdem den Zertifizierungsstellen unmittelbar bekannt zu geben.

Weiterhin wird jährlich eine Übersicht über geeignete Kryptoalgorithmen und zugehörigen Parameter veröffentlicht, die vom Bundesamt für Sicherheit in der Informationstechnik festgestellt werden.

E. Ausblick und internationale Aspekte

Deutschland hat mit dem Signaturgesetz international eine Vorreiterrolle übernommen. Kein anderes Land hat bislang eine vergleichbare Regelung verabschiedet[31].

Deshalb ist es für die vorgesehene Anerkennung von ausländischen Zertifizierungsstellen und Zertifikaten unerläßlich, Rahmenbedingungen zu schaffen, die eine gleichwertige Sicherheit ausweisen.

Bis dahin kann man gesetzlich anerkannte digitale Signaturen mit Kommunikationspartnern im Ausland nur anwenden, soweit diese über Zertifikate deutscher Zertifizierungsstellen verfügen. Es ist vom SigG grundsätzlich nicht verboten, daß deutsche Zertifizierungsstellen im Ausland Annahmestellen für Zertifikatsanträge einrichten und den dortigen Antragstellern Signaturkomponenten aushändigen; dies kann jedoch auf Dauer nur in Einzelfällen helfen.

Eine weiterer Aspekt ist die Gewährleistung der Interoperabilität, ohne die ein rechtssicherer digitaler Datenaustausch nur bedingt möglich sein wird.

F. Besondere Verwaltungsverfahren

Bezüglich des Verwaltungsverfahrens greifen für den Bereich der digitalen Signatur die besonderen Strukturen des TKG nicht. So gelten insbesondere das Beschlußkammersystem und die Zuständigkeit des Beirates nicht für die Vollzugstätigkeiten aus dem Signaturgesetz. Zwar nimmt § 3 SigG auf § 66 TKG Bezug und bestimmt als zuständige Behörde die Regulierungsbehörde für Telekommunikation und Post. Der Bezug auf §

[30] Vgl. Begründung zu § 17 Abs. 4 SigV.
[31] Zum Zeitpunkt der Drucklegung.

66 TKG hat jedoch in diesem Sonderfall gerade nicht zur Folge, daß u.a. die §§ 69 und 73 ff. TKG zur Anwendung kommen. So sind die Beschlußkammern abschließend nur für die in § 73 Abs. 1 TKG aufgeführten Fälle zuständig. Gleiches gilt für die Aufgaben des Beirats, die in § 69 TKG erschöpfend bestimmt sind. Schließlich findet in diesem Zusammenhang auch die verfahrensrechtliche Ausnahmeregelung des § 80 TKG keine Anwendung[32].

Kurz gesagt bedeutet dies: Wird die Reg TP im Rahmen des Signaturgesetzes bzw. der Signaturverordnung tätig, so gelten die allgemeinen Regelungen des Verwaltungsverfahrensgesetz (VwVfG) bzw. die Verwaltungsgerichtsordnung (VwGO).

In der praktischen Anwendung bedeutet dies:

- Ein Vorverfahren nach § 68 Abs. 1 VwGO ist durchzuführen.
- Die Widerspruchsbehörde ist dabei gem. § 73 Abs. 1 S. 2 Nr. 2 VwGO die Regulierungsbehörde.
- Widerspruch und Anfechtungsklage haben gem. § 80 Abs. 1 VwGO aufschiebende Wirkung, allerdings kann die Reg TP die vorläufige Vollstreckbarkeit ihrer Verwaltungsakte nach allgemeinem Verfahrensrecht (§ 80 Abs. 2 VwGO) anordnen.

In der Praxis ist davon auszugehen, daß die Verfahren des einstweiligen Rechtsschutzes nach §§ 80 Abs. 5, 123 VwGO große Bedeutung haben werden.

Auch die Signaturverordnung selbst regelt jedoch Verfahrensvorschriften: So ist abweichend von § 28 Abs. 2 und 3 VwVfG gem. § 1 Abs. 3 SigV in den dort genannten Fällen eine Anhörung stets durchzuführen, um im Hinblick auf die teilweise komplexen organisatorischen und technischen Sachverhalte falsche Entscheidungen auszuschließen.

[32] vgl. Roßnagel MMR 1998, S. 468 ff (S. 473).