



Die zertifizierte Signatur im praktischen Einsatz

Die elektronische Signatur im praktischen Einsatz stellt nicht nur Juristen vor zahlreiche ungeklärte Fragen. Die **digitale Signatur** soll dem Anwender ermöglichen, in elektronischer Form zum Beispiel per eMail rechtsverbindlich sowie „**beweis- und gerichtsfest**“ Erklärungen abzugeben respektive Verträge zu schließen, für die gesetzlich die Schriftform vorgeschrieben ist. Die digitale Signatur wird daher als echte Alternative und Substitut zur Abgabe von Willenserklärungen unter Abwesenden durch Briefpost, per Telefax oder ähnlichen Medien verstanden.

Im Folgenden werden die wichtigsten Begriffe im Zusammenhang mit der Signatur definiert, relevante Vorschriften erklärt und die derzeitigen sowie zukünftigen Anwendungsmöglichkeiten aufgezeigt. Schließlich erfährt der Leser, wie er auf einfache und kostengünstige Weise die elektronische Signatur in seinen vorhandenen Kommunikationsapparat eingliedern kann.

Um das Thema besser verstehen zu können, werden vorab die sieben traditionellen Funktionen der Schriftform erläutert:

1. **Abschlussfunktion:** Durch eine Handlung wird eine rechtsverbindliche Erklärung abgegeben.
2. **Beweisfunktion:** Diese Funktion ist dem bedruckten bzw. beschriebenen Papier immanent und macht die anderen Funktionen nachprüfbar.
3. **Echtheitsfunktion:** Ist als Unterscheidungsmerkmal zu gefälschten Dokumenten zu verstehen.
4. **Identitätsfunktion:** Soll Authentizität, also die eindeutige Identifizierung des Absenders gewährleisten.
5. **Perpetuierungsfunktion:** Im Gegensatz zu mündlich abgegebenen Erklärungen sollen schriftliche Erklärungen lange überprüfbar bleiben.
6. **Verifikationsfunktion:** Das Erfordernis der Nichtabstreitbarkeit bedeutet, dass derjenige, der eine den Anforderungen entsprechende Erklärung abgegeben hat, im nachhinein nicht erfolgreich behaupten kann, eine Erklärung mit diesem Inhalt nicht abgegeben zu haben.
7. **Warnfunktion:** Wer eine Unterschrift unter eine Erklärung setzt, wird deutlich darauf aufmerksam gemacht, dass er eine rechtsverbindliche Erklärung abgibt.

Grundlage der elektronischen Signatur ist die **Verschlüsselungstechnologie**. Ganz wichtig für die folgenden Gedanken ist die Trennung des **zertifizierten Signierungsverfahrens** von der Verschlüsselungstechnologie. Signieren und Verschlüsseln von eMails sind zwei voneinander unabhängige Verfahren, die zwar sinngemäß sehr eng verknüpft sind, jedoch unterschiedliche Zwecke verfolgen. Es sei bemerkt, dass im Bereich der elektronischen Signaturen zwischen den **asymmetrischen und symmetrischen kryptografischen Verfahren** unterschieden wird, ohne hier weitere Einzelheiten ausführen zu wollen. Dienste wie Pretty Good Privacy (**PGP**) oder **GNuPG** (GNU Privacy Guard) verwenden seit Jahren erfolgreich das asymmetrische kryptografische Verfahren zur Verschlüsselung von eMails nebst Anlagen. Dabei wird die Nachricht vom Versender anhand eines dem Empfänger eindeutig zugewiesenen und öffentlich abrufbaren Schlüssels dem öffentlichen Schlüssel (**public key**) verschlüsselt. Diese Nachricht kann dann vom Empfänger mit einem zweiten, dem privaten Schlüssel (**privat key**) entschlüsselt werden. Das Verfahren funktioniert auch in die entgegengesetzte Richtung, indem eine Nachricht mit dem privaten Schlüssel verschlüsselt und vom Empfänger mit dem öffentlichen Schlüssel des Absenders entschlüsselt wird.

Voraussetzung dafür, dass Kommunikationspartner Erklärungen austauschen können, ist lediglich, dass ein Schlüssel öffentlich über das World Wide Web auf einem Server zugänglich ist. Entscheidend ist in diesem Zusammenhang, dass es derzeit technisch ausgeschlossen ist, den privaten Schlüssel aus dem öffentlichen Schlüssel zu errechnen. Der private Schlüssel darf natürlich niemals versendet werden, weil genau dann die Gefahr des Missbrauchs bestünde. Bei den so eben beschriebenen Diensten handelt es sich um Angebote, die den Kommunikationspartnern in erster Linie **Vertraulichkeit** bieten. Mit Vertraulichkeit ist gemeint, dass es für Dritte ausgeschlossen sein soll, den Inhalt der ausgetauschten Daten zur Kenntnis zu bringen. Hier liegt auch der größte Unterschied zwischen der asymmetrischen und der symmetrischen Verschlüsselung. Da bei der symmetrischen Verschlüsselungsmethode der öffentliche und der private Schlüssel identisch sind, ist der Austausch der Schlüssel unsicherer.

Vornehmlicher Sinn und Zweck der **elektronischen Signatur** im Sinne des **Signaturgesetzes (SigG)** ist es, **Authentizität und Integrität** zu gewährleisten. Der Empfänger einer eMail darf /kann/muss sich darauf verlassen können, dass eine signierte eMail mit dem empfangenen Inhalt genauso vom Absender abgegeben wurde, wie sie beim Empfänger angekommen ist. Wenn eine Datei oder eine eMail signiert werden soll, erzeugt die Hard- und Software aus den zu signierenden Daten den so genannten **Hash-Wert**. Der Hash-Wert ist als **digitaler Fingerprint** zu verstehen – ein praktisch einmaliger Wert. Aus dem Hash-Wert können die Daten nicht rekonstruiert werden. Werden die Daten nur geringfügig verändert, ändert sich auch der Hash-Wert. Sollen die Daten versendet werden, wird der errechnete Hash-Wert mit dem privaten – oder falls bekannt – mit dem öffentlichen Schlüssel des Empfängers asymmetrisch verschlüsselt und als Anlage an die elektronische Nachricht und den Daten angefügt. Selbstverständlich ist die Technik der elektronischen Signatur dazu in der Lage, die eigentlichen Daten und nicht nur den Hash-Wert „nebenbei“ zu verschlüsseln, um als Plus zu Authentizität und Integrität auch Vertraulichkeit zu erzeugen.

Nach der Definition von § 2 Abs. 1 Ziff. 1 SigG sind **einfache Signaturen** „*Daten in elektronischer Form, die anderen elektronischen Daten beigelegt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen*“. Die einfache Signatur werden die meisten Leser bereits aus ihren eMail-Clients kennen. Dort besteht in der Regel die Möglichkeit, eine Nachricht mit einer Signatur zu versehen. Diese Form der Signatur gewährleistet nicht viel. Der Beweiswert einer einfach signierten eMail ist vor Gericht gering, wenn nicht weitere Indizien für die Authentizität vorgetragen werden.

Unter einer **fortgeschrittenen Signatur** i.S.v. § 2 Abs. 1 Ziff. 2 SigG sind die Dienste der oben beschriebenen Signaturanbieter, wie PGP zu verstehen. Die Signatur ist „*ausschließlich dem Signaturschlüssel-Inhaber zugeordnet*“, sie wurde „*mit Mitteln erzeugt*“, „*die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann*“, „*die Identifizierung des Signaturschlüssel-Inhabers*“ ist möglich und die „*Daten, auf die sie sich beziehen*“, sind „*so verknüpft ..., dass eine nachträgliche Veränderung der Daten erkannt werden kann*“.

Bei den hier besonders interessierenden **qualifizierten elektronischen Signaturen** i.S.v. § 2 Abs. 1 Ziff. 3 SigG und den **qualifizierten elektronischen Signaturen mit Anbieter-Akkreditierung** i.S.v. § 15 Abs. 1 S. 4 SigG kommen zwei entscheidende Voraussetzungen hinzu. Die qualifiziert zertifizierte elektronische Signatur muss „*auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt*“ worden sein. Um ein Maximum an Authentizität zu garantieren, übernimmt der Staat als Hoheitsträger auf dem Gebiet des wirtschaftlichen und sozialen Zusammenlebens die staatliche Aufsicht und Kontrollfunktion ein. Oberste Aufsichtsbehörde ist die Regulierungsbehörde für Post- und Telekommunikation (RegTep). Bei den qualifizierten elektronischen Signaturen mit Anbieter-Akkreditierung i.S.v. § 15 Abs. 1 S. 4 SigG wird die Sicherheit durch gesetzlich anerkannte fachkundige Dritte gewährleistet.

Nur wer erfolgreich ein umfangreiches Prüfungsverfahren, das in der Signaturverordnung (SigV) festgelegt ist, durchlaufen hat, kann als **Zertifizierungsdiensteanbieter** ein **qualifiziertes Zertifikat** ausstellen. Das qualifizierte Zertifikat wird regelmäßig, aber nicht zwingend auf einer **Chipkarte** mit eingebauten Prozessor gespeichert. Die Kombination aus der Chipkarte und dem Chipkartenlesegerät nennt man **sichere Signaturerstellungseinheit**, welche an den Computer angeschlossen, den Benutzer in die Lage versetzt, elektronische Erklärungen abzugeben, die schriftlichen Erklärungen im klassischen Sinne in nichts nachstehen. Mit den **Signaturanwendungskomponenten** und **den technischen Komponenten für Zertifizierungsdienste** ist das „**System der digitalen Signatur**“ in der Lage, alle Voraussetzungen nach dem Signaturgesetz einzuhalten und den Kommunikationspartnern ca. 98,99 Prozent Vertraulichkeit zu gewährleisten.

Am Beispiel der Rechtsanwälte soll das soeben Dargestellte verdeutlicht werden. Die Rechtsanwaltsammern sind eigenständige Zertifizierungsdiensteanbieter, die zusammen mit der **DATEV** als weiteren Zertifizierungsdiensteanbieter die **KAMMER e:secure** als Signaturkarte anbieten. Beide besitzen als akkreditierte Diensteanbieter das Gütesiegel i.S.v. § 15 SigG. Die DATEV übernimmt die technische Infrastruktur im Sinne des Signaturgesetzes und bietet darüber hinaus Software an für die Kanzleiverwaltung von Großkanzleien bis hin zu maßgeschneiderten Lösungen für kleinere sowie mittlere Kanzleien. Die örtliche Rechtsanwaltskammer kennt ihre Mitglieder und kann deshalb die Identifizierung des Signaturschlüssel-Inhabers und die damit verbundene Erfassung der Pflichtangaben und weiteren **Attribute** einer Signatur zuverlässig vornehmen. Denn entscheidend ist, dass eine Signatur mit Zertifikat anhand eines Verzeichnisses jederzeit (= 30 Jahre?) und zuverlässig dem Signaturschlüssel-Inhaber zugeordnet werden kann. Der Pflichtteil einer **zertifizierten Signatur** liest sich wie folgt: *Der Name oder ein unverwechselbares Pseudonym des Signaturschlüssel-Inhabers, der zugeordnete Signaturprüfchlüssel nebst Bezeichnung der Algorithmen, mit denen der Signaturprüfchlüssel des Signaturschlüssel-Inhabers sowie der Signaturprüfchlüssel des Zertifizierungsdiensteanbieters, eine laufende Nummer des Zertifikates, Beginn und Ende der Gültigkeit des Zertifikates, den Namen des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist, Angaben darüber, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt ist.* Ein **Pseudonym** kann ein Künstlurname sein, ein Firmenname, der auch in einem Handelsregister eingetragen sein sollte oder eben ein plausibler Phantasie name. Ein Pseudonym kann benutzt werden, die Identität Dritten gegenüber geheim zu halten. Es besteht zudem die Möglichkeit, die zertifizierte Signatur mit weiteren Attributen zu versehen. Beispielsweise könnten Rechtsgeschäfte in ihrem rechtlichen und monetären Umfang beschränkt werden. Man könnte auch eine zertifizierte Signatur auf prozessuale Erklärungen beschränken. Es empfiehlt sich als Anwalt, das Attribut Rechtsanwalt in das Zertifikat aufnehmen zu lassen. Zu Recht wird die Signaturkarte der Rechtsanwaltskammer bereits als Königin der Signaturkarten in Deutschland bezeichnet.

Ist die Identifizierung erfolgreich, erhält der Anwalt seinen (europäischen) Anwaltsausweis mit integrierter Chipkarte und dem Kartenlesegerät. Er muss nur noch die Jahresgebühr in Höhe von 65,00 EUR entrichten und ist nun Besitzer einer zertifizierten Signaturkarte, ausgestellt von einem akkreditierten Diensteanbieter. Damit hat er einen unter staatlich kontrollierten Bedingungen erzeugten **Signaturschlüssel** (private key) auf der Chipkarte und einen **Signaturprüfchlüssel** (public key) erhalten. Der Signaturprüfchlüssel wird auf einem vertraulichen Server der DATEV für die Kommunikationspartner öffentlich bereitgehalten. Bevor der Anwalt die Kammer verlassen kann, muss er noch im Sinne von § 5 SigG unterrichtet werden. Dazu ist dem Anwalt eine schriftliche Belehrung auszuhändigen, „*deren Kenntnisnahme dieser durch gesonderte Unterschrift zu bestätigen hat.*“

Nun will der Anwalt die Signaturerstellungseinheit zusammen mit den Signaturanwendungskomponenten erfolgreich in sein Computersystem integrieren. Bei der

Installation eines sicheren Computernetzwerkes in der Rechtsanwaltskanzlei und der Integration der zertifizierten Signatur in den vorhandenen Kommunikationsapparat sollte schon aus haftungsrechtlichen Gründen im Zweifel eine Fachfirma aus der Netzwerksicherheitsdomäne herangezogen werden. Läuft die erforderliche Software, kann der erste Schriftsatz an den Kollegen per elektronischer Post zugestellt werden.

Der Anwalt ruft seine Software auf, den so genannten **GERVA** der Firma DATEV. Der GERVA ist eine eigenständige Applikation, die nicht in vorhandene Office Programme, wie Outlook oder Word eingebunden wird. Es handelt sich um ein Programm mit dem so genannten **IT-TÜV** und übernimmt die Zustellung der elektronischen Dokumente im globalen Netzwerk. Die DATEV bietet zusätzliche Leistungen an, wie z.B. einen **Zeitstempeldienst**, mit dem der genaue Zustellungsauftrag und -empfang bescheinigt werden kann. Vor dem Absenden einer zertifizierten signierten eMail muss der Anwalt stets seine sechsstellige **PIN** in das Kartenlesegerät eingeben. Die Empfänger der zertifizierten eMail müssen sich allerdings den **GERVA-VIEWER (ca. 10 MB)** von den Internetseiten der DATEV herunterladen, um die Signatur zu verifizieren. Für einen Mandanten mit Modem kann dies zu einem langwierigen Prozess werden. Um die Nachricht zu entschlüsseln, ist der Einsatz des GERVA bei der Gegenstelle erforderlich. Der Versand zertifizierter eMails ist ohnehin mehr für den Schriftverkehr mit Gerichten und Behörden oder anderen städtischen Stellen geeignet. Der Vorteil der Rechtsanwaltskammersignaturkarte ist dennoch, dass ein Programm für den Einsatz einer „nur“ fortgeschrittenen Signatur in Microsofts Outlook gleich von der DATEV auf einer CD-ROM mitgeliefert wird. Für die Korrespondenz mit den Mandanten wird der Einsatz einer fortgeschrittenen Signatur in den meisten Fällen ausreichend sein.

Kommt es nun zu einem echten Prozess und legt der Anwalt beispielsweise seine mit einer zertifizierten Signatur versehene eMail als Beweismittel vor, gilt für ihn gemäß **§ 292a Zivilprozessordnung (ZPO)** mit Verweis auf **§ 126a Bürgerliches Gesetzbuch (BGB)** der Anscheinsbeweis dafür, dass die eMail mit zertifizierter Signatur die oben beschriebenen sieben Funktionen eines Schriftstückes zu Gunsten des Erklärenden erfüllt. Der Beweisgegner, der erfolgreich bestreiten will, muss konkrete Tatsachen vortragen, die Zweifel an der Authentizität der Signatur aufkommen lassen. Beispiele dafür wären Nachweise darüber, dass die Signaturerstellungseinheit im Zeitpunkt der Erstellung nicht den Anforderungen entsprach oder dass der Zertifizierungsdiensteanbieter nicht die Vorschriften des Signaturgesetzes und/oder -verordnung eingehalten hat. Dieser Nachweis wird allerdings nur selten gelingen und die Ausnahme bleiben. Für den Juristen wäre es wünschenswert, dass die Amts- und Landgerichte, die Finanz-, Verwaltungs- und Sozialgerichte es dem Bundesgerichtshof schnellstmöglich gleichmachen und den Schriftverkehr per elektronischer Post zulassen würden. Das Mahnverfahren kann bereits online per signierter eMail betrieben werden.

Die Anforderungen an die Zertifizierungsdiensteanbieter werden in diesem Kontext bewusst weggelassen. Wichtig ist, dass der Endanwender als Signaturschlüssel-Inhaber einen Diensteanbieter mit Zertifikat im Sinne des Signaturgesetzes wählt. Für alle Beteiligten lassen die Vorteile aus ökonomischer und ökologischer Betrachtungsweise kein längeres Warten mehr zu. Der Einsatz zertifizierter elektronischer Signaturen ist nicht nur für Juristen von Vorteil. Für Steuerberater und Makler, Vereine und Verbände, Kaufleute oder Handwerker und all diejenigen, die über das Internet Waren oder Dienstleistungen vertreiben, kann der Einsatz von zertifizierten Signaturen gewinnbringend und im Streitfalle von entscheidender Bedeutung sein. Die Anwendungsmöglichkeiten für qualifizierte Signaturen sind zahlreich. Exemplarisch seien hier nur Steuererklärungen, Mahnverfahren, Kfz-Anmeldungen oder Einwohnermeldeamtsachen genannt, die in Zukunft mittels Signatur elektronisch von jedem Ort der Welt erledigt werden könnten. Wer nicht in den Genuss einer Signaturkarte der Rechtsanwaltskammer kommt, kann auf weitere Anbieter zurückgreifen. Last but not least wird auf das **eGovernmentprogramm BundOnline2005** hingewiesen. Dort werden neben aktuellen Anwendungsmöglichkeiten wünschenswerte Visionen aufgezeigt, die rasch Wirklichkeit werden sollten.

Nutzungshinweis für Kartenlesegerät mit JAVA-Anwendungen

Wer mit der Signaturkarte der Rechtsanwaltskammer und installierter DATEV-Software (Sicherheitspaket) über einen Browser online einen Mahnbescheid beantragen möchte, der steht vor dem Problem, dass die JAVA-Applikation das Kartenlesegerät nicht ohne weiteres erkennt - solange der DATEV-Dienst **DVckService.exe** nicht manuell beendet wurde, kann ein Mahnantrag nicht signiert werden.

Folgende Vorgehensweise wird daher empfohlen:

1. Beenden Sie das DATEV-Sicherheitspaket - sofern geöffnet.
2. Über den Task-Manager oder die Systemsteuerung/Computerverwaltung/Dienste den Dienst **DVckService.exe** beenden.
3. Nun kann die JAVA-Applikation im Browser gestartet werden und das Kartenlesegerät wird erkannt.
4. Wenn der Arbeit im Browser beendet ist und die JAVA-Applikation geschlossen wurde, sollte der Dienst **DVckService.exe** erneut manuell gestartet werden; anderenfalls funktioniert das DATEV-Sicherheitspaket nicht reibungslos.

Bei Rückfragen und zum Testen der Signatur, können Sie mir gern ein signierte eMail an dpms@sevriens.net schicken.