Volker Gruhn/Vincent Wolff-Marting
André Köhler/Christian Haase
Torsten Kresse

Elektronische Signaturen in modernen Geschäftsprozessen

Volker Gruhn/Vincent Wolff-Marting
André Köhler/Christian Haase
Torsten Kresse

Elektronische Signaturen in modernen Geschäftsprozessen

Schlanke und effiziente Prozesse mit der eigenhändigen elektronischen Unterschrift realisieren

Mit 25 Abbildungen

vieweg

Bibliografische Information Der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.d-nb.de> abrufbar.

1. Auflage März 2007

Lektorat: Günter Schulz / Andrea Broßler

Der Vieweg Verlag ist ein Unternehmen von Springer Science+Business Media.
www.vieweg.de

Umschlaggestaltung: Ulrike Weigel, www.CorporateDesignGroup.de
Umschlagbild: Nina Faber de.sign, Wiesbaden
Druck- und buchbinderische Verarbeitung: MercedesDruck, Berlin
Printed in Germany

ISBN 978-3-8348-0268-2

Vorwort

Kostensenkungen, Effizienzsteigerungen und die Erhöhung der Flexibilität hinsichtlich zukünftiger Anforderungen ist ein allgegenwärtiges und wichtiges Thema bei der Gestaltung und Verbesserung von Geschäftsprozessen. Um diese Ziele zu erreichen, sind viele verschiedene Maßnahmen denkbar, die in Abhängigkeit von der jeweiligen Beschaffenheit des Unternehmens und der Situation in den relevanten Märkten ausgewählt und gestaltet werden können.

Die Vermeidung von Papierdokumenten in geschäftlichen Abläufen kann dazu einen wichtigen Beitrag leisten. Dies wird vielfach schon erfolgreich durchgeführt. Jedoch müssen bestimmte Dokumente aus rechtlichen oder organisatorischen Gründen mit Unterschriften versehen sein. In diesen Fällen ist die Verwendung eines elektronischen Äquivalents nicht ohne weiteres möglich. Für den Druck, die Bereitstellung, den Transport, die Auswertung und die Archivierung solcher Dokumente entstehen oft erhebliche Kosten. Die Potenziale moderner Informationstechnologie können in solchen Fällen nicht oder nur sehr begrenzt genutzt werden.

Um solche unterschriftsbehafteten Dokumente, statt in Papierform, in elektronischer Form zu verwenden, sind vier wesentliche Komponenten nötig. Es werden zunächst ausreichende rechtliche Grundlagen für eine solche Substitution benötigt, es werden technische Voraussetzungen zur Realisierung der Substitution gebraucht, es müssen organisatorische Veränderungen in den Geschäftsprozessen stattfinden und es muss sichergestellt werden, dass die beteiligten Personen die geschaffene technische Lösung akzeptieren und benutzen.

Die rechtlichen Grundlagen und die technischen Voraussetzungen wurden in den vergangenen Jahren geschaffen. Damit ist nun eine wichtige Basis vorhanden, auf der Unternehmen aufbauen können. Die bisherige händische Unterschrift kann durch eine elektronische Signatur ersetzt werden. Das so erzeugte elektronische Dokument hat (unter bestimmten Voraussetzungen) die gleiche Beweiskraft wie ein unterschriebenes Papierdokument.

Jedoch ist zu beobachten, dass die Umsetzung elektronischer Signaturen in Unternehmensprozessen nur zögerlich erfolgt. Entscheider sehen sich in diesem Thema mit einer ganzen Reihe von Unsicherheiten konfrontiert. Dazu gehören Fragen zu den nötigen Umgestaltungen der Geschäftsprozesse, zu den nötigen Investitionssummen, zu den zu erwartenden Vorteilen, zu Wirtschaftlichkeitsberechnungen, zur Akzeptanz der Technologie durch Mitarbeiter und Kunden und vieles mehr. Das nötige Know-How zur Beantwortung dieser Fragen ist in den Unternehmen oft nicht vorhanden. Gleichzeitig handelt es sich um ein sehr komplexes Thema, das sehr viele rechtliche und technische Varianten zulässt, aus denen eine Auswahl erfolgen muss.

Das vorliegende Buch soll in diesen und vergleichbaren Situationen eine Unterstützung bieten. Dazu wird der aktuelle Stand der rechtlichen und technischen Grundlagen und Möglichkeiten anschaulich erläutert. Darüber hinaus wird gezeigt, welche Besonderheiten sich aus den betroffenen Geschäftsprozessen heraus ergeben können und wie Lösungsmöglichkeiten dafür aussehen. Dieses Buch ist deshalb als Praxishandbuch für Entscheider, Projektmanager, Prozessdesigner, aber durchaus auch für Studenten geeignet, die sich aus einer praxisnahen Sicht dem Thema der elektronischen Signatur nähern wollen.

Die Autoren Prof. Dr. Volker Gruhn, Vincent Wolff-Marting, André Köhler, Christian Haase und Torsten Kresse waren gemeinsam in verschiedenen Projekten bei deutschen Versicherern und Finanzdienstleistern zur Einführung der elektronischen Signatur beratend beteiligt. Die Kenntnis der Probleme, der aufgetretenen Schwierigkeiten, der relevanten Geschäftsprozesse uvm. aus diesen Projekten haben entscheidend zum Aufbau und zur inhaltlichen Gestaltung des vorliegenden Buches beigetragen.

Leipzig, im Januar 2007

Prof. Dr. Volker Gruhn

Vincent Wolff-Marting

André Köhler

Christian Haase

Torsten Kresse

Inhaltsverzeichnis

1 Einführung und Überblick

1.1 Ziel des Buches

Elektronische Signaturen sind ein wichtiges Thema in der deutschen Wirtschaft und der Verwaltung. Die enormen Nutzenpotenziale sind erkannt, jedoch bereitet deren Erschließung noch Schwierigkeiten. Die Gründe dafür liegen neben dem oft noch fehlenden Know-How in den Unternehmen und Behörden vor allem in der Notwendigkeit, traditionelle Geschäftsprozesse zu überdenken und ggf. neu zu erarbeiten. Dennoch ist absehbar, dass schon in naher Zukunft der Einsatz elektronischer Signaturen zu einem Standard in der deutschen Wirtschaft heranwachsen wird.

Viele Unternehmen starten auf diesem Gebiet bereits die ersten Pilotprojekte, andere haben dies für die nahe Zukunft geplant. Die Motivation dafür ist das hohe Einsparungspotenzial durch automatisierte und beschleunigte Geschäftsprozesse, das der Einsatz elektronischer Signaturen nach der Überwindung aller rechtlichen, technischen und organisatorischen Hürden verspricht. Der standardisierte, rechtssichere Austausch elektronischer Information zwischen den Unternehmen, Institutionen und Kunden wird damit ebenso möglich, wie die Umstellung auf vollständig elektronische Geschäftsprozesse und das weitgehend papierlose Büro.

Dieses Buch gibt Antworten auf viele Fragen, die bei der Einführung elektronischer Signaturen und der Weiterverarbeitung elektronisch signierter Dokumente auftreten können. Dabei werden neben fachlichen und technischen Lösungsvorschlägen auch rechtliche Hinweise gegeben. Darüber hinaus werden spezifische Prozesse bei der Erstellung und Weiterverarbeitung elektronischer Signaturen und elektronisch signierter Dokumente betrachtet. Die Ergebnisse werden so aufbereitet, dass die Erkenntnisse sofort in eigene Projekte übertragen werden können.

1.2 Wer soll dieses Buch lesen?

Dieses Buch wendet sich vorrangig an Praktiker, Entscheidungsträger und IT-Planer, die in oder für Unternehmen an Projekten zur Einführung der elektronischen Signatur arbeiten oder arbeiten werden. Das Buch ist so aufgebaut, dass kaum Vorkenntnisse vorausgesetzt werden. Neben einer kurzen Einführung in die Thematik und einem rechtlichen und technischen Überblick wer-

den gezielt Aspekte vorgestellt, die bei der Einführung der elektronischen Signatur in Geschäftsprozesse eine Rolle spielen.

Durch seine modulare Struktur bietet das Buch die Möglichkeit, die vorgestellten Aspekte schnell und einfach in die Planung und Durchführung eigener Projekte einfließen zu lassen. Indem es die Anforderungen aller betroffenen Entscheidungsträger betrachtet, kann es zu einer besseren Kommunikation zwischen Geschäftsführung, IT-Abteilung und Mitarbeitern beitragen.

1.3 Aufbau des Buches

Zunächst werden in Kapitel 2 die rechtlichen Grundlagen beschrieben, die in der Vergangenheit für den Einsatz der elektronischen Signatur geschaffen wurden. Dazu werden zunächst die gesetzlichen Formvorschriften erläutert, die eine Unterschrift ggf. nötig machen. Es werden weiterhin die Kategorien der Sicherheit erläutert, die mit elektronischen Signaturen realisiert werden können. Dazu gehören die einfache, die fortgeschrittene und die qualifizierte Signatur. Darüber hinaus wird das deutsche Recht mit der internationalen rechtlichen Situation verglichen. Im Anschluss daran werden die Funktionen einer Unterschrift erläutert. Weiterhin wird gezeigt, welche Beweisqualität elektronisch signierte Dokumente im Vergleich zu Papierdokumenten haben.

Im Kapitel 3 werden die informationstechnischen Grundlagen beschrieben, mit denen sich elektronische Signaturen realisieren lassen. Dazu werden zunächst zentrale Themen wie verschiedene Verschlüsselungsverfahren, Hashverfahren, Zertifikate und Zeitstempel erläutert. Im Anschluss daran wird der typische Ablauf des elektronischen Signierens und Verifizierens dargelegt. Der Schwerpunkt der Betrachtung liegt dabei auf den fortgeschrittenen Signaturen, auf fortgeschrittenen zertifikatsbasierten Signaturen und auf qualifizierten Signaturen. Weiterhin wird gezeigt, welche Verfahren zur Anwendung kommen können, um den Signaturschlüssel zu schützen. Dabei werden insbesondere die biometrischen Verfahren erläutert. Der letzte Teil dieses Kapitels ist der Verwendung von biometrischen Merkmalen innerhalb von Signaturen gewidmet. Es wird beschrieben, wie solche Merkmale in Signaturen integriert und später verifiziert werden können.

Die Umsetzung der elektronischen Signaturen in Geschäftsprozessen ist Gegenstand des Kapitels 4. Dazu werden zunächst die Nutzenpotenziale elektronischer Signaturen für unternehmerische Zwecke erläutert. Anschließend erfolgt eine Betrachtung der Einsatzszenarien in der unternehmensexternen und -internen Kommunikation. Weiterhin werden ausgewählte Realisierungsaspekte dargelegt, die besonders in geschäftlichen Situationen von Bedeutung sind. Dazu gehören Mehrfachsignaturen, gemeinsame Signaturen, Zeitstempelsignaturen, Zeitspannensignaturen, automatisierte Massensignaturen, bestimmte Verifizierer sowie die Signatur von Datenströmen. Der letzte Teil

dieses Kapitels ist der Archivierung elektronisch signierter Dokumente gewidmet, da dies ein sehr wichtiges Thema für unternehmerische Belange ist, das jedoch oft vernachlässigt wird. Es werden dazu zunächst die wichtigsten Dokumentations- und Aufbewahrungsvorschriften für Unternehmen erläutert. Es wird anschließend erklärt, wann Algorithmen zur Erstellung von Signaturen ihre Sicherheitseignung verlieren können und welche Auswirkungen dies auf bereits signierte Dokumente hat. Weiterhin werden die gesetzlichen Anforderungen an die Langzeitarchivierung solcher Dokumente beschrieben. Schließlich wird ein Konzept zur Realisierung einer derartigen Archivierung vorgestellt und in einzelnen Aspekten erläutert. Dazu gehört die Auswahl geeigneter Nutzdatenformate, die Archivierung von Verifikationsdaten, die Erneuerung von Signaturen, die Transformation elektronischer Dokumente sowie die Erneuerung der Datenträger in einem Archivsystem.

Gegenstand des Kapitels 5 ist eine Fallstudie, anhand derer gezeigt wird, wie die konkrete Ausgestaltung und Umsetzung der elektronischen Signatur in einem Geschäftsprozess erfolgen kann. Als Anwendungsbeispiel wurde dazu die Erstellung von elektronisch signierten Versicherungsanträgen am Point of Sale ausgewählt. Die Vorgehensweise, die der Realisierung dieses Szenarios zu Grunde liegt, sowie die gewonnenen Erkenntnisse daraus können auch auf andere Prozesse übertragen werden. Zunächst werden die rechtlichen Grundlagen des Prozesses erläutert. Anschließend wird gezeigt, wie die fachliche Anforderungsanalyse und Prozessmodellierung vorgenommen werden kann. Schließlich erfolgt die Beschreibung der technischen Realisierung entsprechend der zuvor formulierten fachlichen Anforderungen. Darüber hinaus wird gezeigt, welche Angriffsszenarien innerhalb dieses Prozesses denkbar sind, die auf eine Kompromittierung der Dokumente oder Systeme abzielen könnte und wie die dazu passenden Schutzmechanismen aussehen.

Das Buch schließt durch Kapitel 6 mit einer Zusammenfassung und gibt einen kurzen Ausblick über die zukünftig zu erwartenden Entwicklungen.

2 Rechtliche Grundlagen der elektronischen Signatur

Dieses Buch behandelt die Frage, wie elektronische Signaturen manuelle Unterschriften ersetzen können. Bevor jedoch die elektronische Signatur untersucht wird, soll an dieser Stelle zunächst die Anwendung der Unterschriften im Rechtsverkehr analysiert werden.

2.1 Die Unterschrift als Teil gesetzlicher Formvorschriften

Formzwang und Formfreiheit

Die meisten Willenserklärungen und Verträge unterliegen der *Formfreiheit*, das heißt, es steht den Handelnden völlig frei, sich auf eine geeignete Form zu einigen – sei sie nun handschriftlich, gedruckt, elektronisch, mündlich, telefonisch oder auch durch Handschlag. Nur in wenigen Fällen ist gesetzlich eine besondere Form vorgeschrieben. Das bürgerliche Gesetzbuch unterscheidet folgende gesetzliche Formen:

- Textform [Bunc, § 126b]
- Schriftform [Bunc, § 126]
- elektronische Form [Bunc, § 126a]
- notarielle Beurkundung [Bunc, § 128]
- öffentliche Beglaubigung [Bunc, § 129]

Textform

Die *Textform* verlangt eine Urkunde oder eine andere „zur dauerhaften Wiedergabe in Schriftzeichen“ [Bunc, § 126b] geeignete Erklärung. Die *Person des Erklärenden* muss genannt sein und der Abschluss der Erklärung erkennbar gemacht werden. Eine Unterschrift wird nicht verlangt. Neben der Papierurkunde kommen auch elektronische Dateien oder ähnliches in Frage. Flüchtige Formen, insbesondere (fern-)mündliche Erklärungen sind ausgeschlossen. Als flüchtig sind in diesem Zusammenhang auch Computermeldungen zu sehen, die zwar vom Benutzer gelesen, nicht aber gedruckt und gespeichert werden können. Durch den Verzicht auf eine Unterschrift fehlt eine Identifikationsmöglichkeit des Erklärenden und ein klarer räumlicher Abschluss des Dokumentes. Die Identifikation wird üblicherweise durch Nennung des Namens gewährleistet sein. Der Dokumentenabschluss kann durch das Bild einer Unterschrift oder durch eine Floskel wie *„Diese Erklärung ist ohne Unterschrift gültig“*, *„gez. Name“*, eine Grußformel, das Wort *Ende* oder ähnliches erreicht werden [Nis01, S. 56ff], [HKJ$^+$04, § 126b Rn 31f].

Schriftform

Zur Erfüllung der *Schriftform* wird eine eigenhändige Namensunterschrift unter einem Dokument verlangt [Bunc, § 126]. Dazu muss das Dokument physisch vorliegen. Elektronische Dokumente wären dafür ungeeignet, auch eine telekommunikative Übertragung des unterschriebenen Dokumentes wäre nicht möglich. Bis auf wenige Ausnahmen darf die Schriftform allerdings durch die *elektronische Form* ersetzt werden, die diese Einschränkungen

überwindet. Ausdrücklich ausgenommen sind beispielsweise Verbraucherdarlehensverträge, Kündigungen und Aufhebungen eines Arbeitsverhältnisses, Bürgschaftserklärungen, abstrakte Schuldversprechen sowie Schuldanerkenntnisse [HKJ+04, § 126 Rn 166]. Nach herrschender Meinung muss ferner der Empfänger mit dem Ersatz einverstanden sein [HKJ+04, § 126 Rn 167]. Eine *notarielle Beurkundung* ist als Ersatz immer möglich [HKJ+04, § 126 Rn 3].

elektronische Form

Die *elektronische Form* erfordert „eine qualifizierte elektronische Signatur nach dem Signaturgesetz“ [Bunc, § 126a]. Eine Erläuterung der qualifizierten Signatur erfolgt in Kapitel 2.2.3. Wie schon bei der Textform muss auch hier der Aussteller der Erklärung seinen Namen angeben.

notarielle Beurkundung und öffentliche Beglaubigung

Notarielle Beurkundung und *öffentliche Beglaubigung* werden von Notaren vorgenommen [Bunc, §§ 128f]. Dieses komplexe Feld ist für die weiteren Ausführungen dieses Buchs nicht von Belang und wird daher nicht tiefer behandelt.

vereinbarte Formen

Ob für einen konkreten Anwendungsfall eine besondere Form notwendig ist, ist im Einzelfall zu untersuchen. Eine Übersicht über die Situationen, in denen die Textform vorgeschrieben ist, findet sich beispielsweise bei Nissel [Nis01, S. 66-79]. Neben den gesetzlich vorgeschriebenen Formen können Vertragsparteien freiwillig untereinander für Nachrichten oder Erklärungen bestimmte Formen verbindlich vereinbaren. Das Bürgerliche Gesetzbuch definiert drei Ausprägungen der sogenannten *vereinbarten Form* [Nis01, S. 33]:

- Die *vereinbarte Textform* [Bunc, § 127 Abs. 1] entspricht der Textform.
- Die *vereinbarte Schriftform* [Bunc, § 127 Abs. 1 und 2] entspricht der Schriftform, erlaubt auch eine telekommunikative Übermittlung ohne Unterschrift, beispielsweise per Telefax.
- Die *vereinbarte elektronische Form* [Bunc, § 127 Abs. 1 und 3] entspricht der elektronischen Form, erlaubt darüber hinaus auch einfache und fortgeschrittene Signaturen (siehe Kapitel 2.2.1 und 2.2.2).

Im Vergleich zu den jeweils entsprechenden gesetzlichen Formen sind die Bestimmungen gelockert, „soweit nicht ein anderer Wille [einer Vertragspartei] anzunehmen ist“ [Bunc, § 128 Abs. 2 sowie 3]. Allerdings steht es den Vertragsparteien frei, auch völlig andere Formen zu vereinbaren, soweit dem nicht eine Rechtsvorschrift entgegensteht. Unzulässig werden im Zweifel alle Formvereinbarungen sein, die die schwächere Partei benachteiligen (vgl. z. B. [Bunc, § 574b] siehe weiterführend [HKJ+04, § 127 Rn 9ff]).

Konkrete Anforderungen an elektronische Signaturen sind im Signaturgesetz [Bunk] und der Signaturverordnung [Bunl] festgelegt. Der Gesetzgeber hat unterschiedliche, aufeinander aufbauende Kategorien für elektronische Signaturen vorgesehen: die einfache, die fortgeschrittene und die qualifizierte Signatur. Zusätzliche Sicherheit kann durch Akkreditierung der Aussteller qualifizierter Signaturen erreicht werden. In Kapitel 2.2 wird konkret dargestellt, wie mit steigenden technischen Anforderungen an die Signaturen auch ihre

Anwendungsmöglichkeiten wachsen. Der Beweiskraft einer elektronischen Signatur kommt eine besondere Bedeutung zu. Sie muss ausreichend hoch sein, um nötigenfalls auch vor Gericht die Gültigkeit einer Willenserklärung sicherstellen zu können.

2.2 Kategorien der Sicherheit mit elektronischen Signaturen

2.2.1 Die einfache elektronische Signatur

Definition

Elektronische Signaturen im Sinne des Gesetzes sind „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“ [Bunk, § 2 Nr. 3]. Für einfache elektronische Signaturen bestehen keine Anforderungen bezüglich der Fälschungssicherheit oder der nachvollziehbaren Zuordnung einer Signatur zu einer Person. Es werden insbesondere auch keine Mechanismen verlangt, die ein nachträgliches Verändern des unterzeichneten Dokuments verhindern. Unterschriften, die als Bild eingescannt unter ein Dokument gesetzt werden, fallen beispielsweise in diese Kategorie [Nis01, S. 45]. Aber auch die „bloße Absenderangabe in einem E-Mail“ [HKJ+04, § 126a Rn 20] kann eine einfache Signatur sein.

Allerdings können einfache Signaturen durchaus sicher sein. Es ist selbstverständlich möglich, auch in dieser Kategorie Verschlüsselungen einzusetzen, die das Sicherheitsniveau steigern. Unabhängig von den möglichen Schwächen einfacher elektronischer Signaturen sind sie grundsätzlich als Beweismittel geeignet (siehe [Das00, Art. 5 Abs. 2]) und rechtsgültig. Sofern der Erklärende namentlich benannt ist, erfüllen Dokumente mit einer einfachen elektronischen Signatur die Anforderungen der *Textform*.

2.2.2 Die fortgeschrittene elektronische Signatur

Definition

Fortgeschrittene elektronische Signaturen sind einfache Signaturen mit einigen Erweiterungen. Sie müssen untrennbar mit dem Dokument, auf das sie sich beziehen, verknüpft sein. Nachträgliche Änderungen des Dokumentes müssen nachweisbar sein und es darf nicht möglich sein, eine vorhandene Signatur einfach auf ein anderes Dokument zu übertragen. Fortgeschrittene Signaturen müssen eine Identifizierung des Unterzeichners ermöglichen. Dazu sollen die Mittel, die zur Erstellung einer fortgeschrittenen elektronischen Signatur erforderlich sind, unter der alleinigen Kontrolle des Unterzeichners stehen [Bunk, § 2 Nr. 2].

Produkte

Fortgeschrittene elektronische Signaturen können mit wenig Aufwand durch handelsübliche Personalcomputer erstellt werden. Geeignete Softwareprodukt-

te sind zum Beispiel *GNU Privacy Guard* oder *Pretty Good Privacy*[1] [Gei03, S. 17]. Diese und ähnliche Produkte erzeugen die Signatur mittels eines kryptografischen Schlüssels, der im Besitz des Unterzeichners ist. Solche Schlüssel sind lange Bitfolgen, die auf einer Festplatte, einer Diskette oder einer Smartcard gespeichert sind. Anders als bei der im folgenden Kapitel beschriebenen qualifizierten elektronischen Signatur, hat der Gesetzgeber keinerlei Vorschriften bezüglich des Schlüssels oder seiner Speicherung erlassen.

Biometrische Merkmale in fortgeschrittenen Signaturen

Alternativ zur Authentifizierung des Unterzeichners durch den Besitz eines Schlüssels können auch biometrische Merkmale in die Signatur einfließen. So können auch digitalisierte eigenhändige Unterschriften fortgeschrittene elektronische Signaturen sein. Eine eigenhändige Unterschrift identifiziert den Unterzeichner, da nur er zu ihrer Erzeugung fähig ist. Die biometrischen Merkmale müssen untrennbar mit dem Dokument verknüpft werden. Eine Übertragung der Unterschrift auf andere Dokumente darf nicht möglich sein, ferner müssen Manipulationen am Dokument die Unterschrift ungültig machen [LS04, S. 94].

Anwendungsfelder

Die Beweisqualität fortgeschrittener elektronischer Signaturen ist stärker ausgeprägt, als jene einfacher Signaturen, trotzdem sind die Anwendungsfelder grundsätzlich ähnlich: Für alle formfreien Rechtsgeschäfte sind fortgeschrittene elektronische Signaturen einsetzbar, die in besonderen Fällen verlangte Schriftform wird allerdings nicht erfüllt.

2.2.3 Die qualifizierte elektronische Signatur

Definition

Qualifizierte elektronische Signaturen erfüllen zuvorderst alle Eigenschaften und Anforderungen fortgeschrittener (und damit auch einfacher) Signaturen. Bei der Erzeugung einer qualifizierten elektronischen Signatur müssen sichere Signaturerstellungseinheiten verwendet werden und die Signaturen müssen auf qualifizierten Zertifikaten beruhen [Bunk, § 2 Nr. 2].

Signaturerstellungseinheit

Die *sichere Signaturerstellungseinheit* enthält den Signaturschlüssel. In der Praxis erfüllen *Smartcards* diesen Zweck. Um den Schlüssel nutzen zu können, muss sich der Unterzeichner zunächst wahlweise durch Wissen (z. B. Pin oder Passwort) und den Besitz eines Gegenstandes (meist ist die Signaturerstellungseinheit selber dieser Gegenstand) oder durch biometrische Merkmale (z. B. Fingerabdruck, Unterschrift) und den Besitz eines Gegenstandes legitimieren [Bunl, § 15 Abs. 1]. Nach erfolgter Legitimation nimmt die Signaturerstellungseinheit die eigentliche Signierung vor, ohne dabei den Schlüssel preiszugeben. Der Unterzeichner muss erkennen können, was er signieren wird. Fälschung der Signaturen oder Verfälschung signierter Daten müssen zuverlässig nachvollziehbar sein [Bunk, § 17], [Bunl, § 15].

[1] Pretty Good Privacy (PGP) ist eine Produkt der PGP Corporation; weitere Informationen unter [PGP]. GNU Privacy Guard (GnuPP) ist eine Open Source Alternative mit vergleichbarem Funktionsumfang; Informationen unter [Fre]. Siehe auch [Bun04a, S. 2531f].

Zertifizierungsstellen

Das Konzept qualifizierter elektronischer Signaturen sieht eine unabhängige Stelle vor, der sowohl der Unterzeichner, als auch alle, die sich auf die Signatur verlassen oder berufen wollen, vertrauen müssen. Diese Funktion erfüllen private Dienstleister, die als *Zertifizierungsstellen*, *Zertifizierungsdienstanbieter*, *certification authority* (*CA*) oder auch *Public Key Infrastructure* (*PKI*) bezeichnet werden. In der kryptografischen Forschung werden solche Stellen auch einfach als *vertraute Dritte* (*Trusted Third Party*) bezeichnet [MOV96, S. 30].

Zertifikate

Diese Zertifizierungsstellen sind für die Vergabe *qualifizierter Zertifikate* zuständig. Ein Zertifikat muss bestimmte Angaben enthalten – beispielsweise den Namen des Inhabers, Angaben zum Signaturschlüssel und zum Gültigkeitszeitraum des Zertifikates [Bunk, § 7]. Vor der Erstellung eines Zertifikates wird die Identität des künftigen Zertifikatinhabers anhand von Ausweispapieren geprüft. Einmal ausgestellte Zertifikate müssen jederzeit und für jedermann über öffentliche Kommunikationskanäle auf ihre Echtheit geprüft werden können. Diese Möglichkeit muss die Zertifizierungsstelle für mindestens fünf Jahre über die Gültigkeitsdauer des Zertifikates hinaus sicherstellen [Bunl, § 4] – in besonderen Fällen sogar 30 Jahre (siehe hierzu Kapitel 2.2.4).

Anwendungsfeld

Die qualifizierte elektronische Signatur hat „im Rechtsverkehr die gleiche Wirkung [...] wie eine eigenhändige Unterschrift“ [Bunk, § 6 Abs. 2]. Insbesondere kann sie die Schriftform ersetzen, die für besondere Rechtsgeschäfte vorgeschrieben ist [Bunc, § 126]. Der Beweiswert einer qualifizierten Signatur ist deutlich höher als der einer Unterschrift auf Papier: Sofern nicht das Gegenteil glaubhaft gemacht werden kann, gilt eine qualifiziert signierte Willenserklärung im Zivilrecht als authentisch [Bung, §§ 371a, 440] (vormals auch [Bunh, § 292a]). Eine herkömmliche Unterschrift dagegen kann jederzeit angefochten werden, solange ihre Echtheit nicht in vollem Umfang nachgewiesen ist [Nis01, S. 34], [Bung, § 439].

Zugelassene Algorithmen

Die *Bundesnetzagentur* (vormals *Regulierungsbehörde für Telekommunikation und Post*, *RegTP*) prüft fortlaufend die Eignung von Signaturalgorithmen und veröffentlicht mindestens einmal jährlich eine Studie mit den Ergebnissen (siehe [Bun06b]). Der Gesetzgeber geht davon aus, dass nur für einen begrenzten Zeitraum Prognosen über die Zuverlässigkeit von Signaturalgorithmen möglich sind. Für qualifizierte elektronische Signaturen sind nur solche Algorithmen zugelassen, deren Eignung für die kommenden sechs Jahre als gesichert gilt. Qualifizierte Zertifikate dürfen maximal fünf Jahre gültig sein [Bunk, § 14 Abs. 3]. Unabhängig davon bleiben einmal getätigte qualifizierte elektronische Signaturen auch über diesen Zeitraum hinaus gültig. Es kann allerdings sein, dass ihre Beweiskraft durch einen erfolgreichen Angriff gegen die verwendeten Algorithmen in Frage gestellt wird. Im Abschnitt 5.4.8 wird diese Herausforderung aufgegriffen. Die technischen Forderungen für qualifizierte elektronische Signaturen sind im Anhang der Signaturverordnung [Bunl] festgehalten.