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.

3 Technische Realisierung elektronischer Signaturen

3.1 Informationstechnische Grundlagen

3.1.1 Verfahren zur Verschlüsselung

Kryptographie

Die elektronische Signatur beruht auf kryptografischen Verfahren, deren Kern die Verschlüsselung ist [MOV96, S. 4]. Verschlüsselung wandelt anhand bestimmter Verfahren (*Verschlüsselungsalgorithmen*) eine Klartext-Nachricht in einen *Geheimtext* (*Chi rat*) um [Bun04b, S. 15]. In die Berechnung fließt ein geheimer Parameter, der *Schlüssel*, ein. Die Entschlüsselung als Umkehrung des Verfahrens ist wiederum nur unter Verwendung eines Schlüssels möglich. Ohne Kenntnis des Schlüssels sollte der Geheimtext für einen Betrachter keine Rückschlüsse auf den Klartext zulassen. Ferner ist es ohne Schlüssel unmöglich, die verschlüsselte Nachricht zielgerichtet zu verändern. Ungerichtete Veränderungen, die darauf abzielen, die Kommunikation zu stören, werden für gewöhnlich nicht unterbunden.

Kerckhoffs-Prinzip

Viele historische Verschlüsselungsverfahren erforderten eine Geheimhaltung des Verfahrens selber. Wenn sichere Kommunikation mit einem offenen und wechselnden Kreis von Personen möglich sein soll, kann es nicht zweckmäßig sein, für jeden Kommunikationspfad ein eigenes Verfahren zu entwerfen, auszuhandeln und für den späteren Einsatz bereitzuhalten. Der Philologe Auguste Kerckhoffs von Nieuwenhof formulierte bereits 1883, dass die Veröffentlichung des Verfahrens für dessen Verlässlichkeit nicht hinderlich sein darf [Jun02, S. 8]. Die Sicherheit moderner Verschlüsselungsalgorithmen wird daher nicht durch ihre Geheimhaltung gewährleistet. Im Gegenteil: Viele Verfahren sind offengelegt. So kann sich jedermann von ihrer Wirkungsweise überzeugen. Schwachstellen können gefunden werden. Diese ständige Kontrolle ist notwendig und sinnvoll, da es bisher nicht gelungen ist, ein Verfahren zu entwickeln, dass praktikabel genutzt werden kann und dessen Sicherheit mathematisch bewiesen werden kann [MOV96, S. 9] [Sch01a, S. 82].[2]

Die Sicherheit dieser Verfahren hängt folglich wesentlich von der Geheimhaltung der verwendeten Schlüssel ab. Sie dürfen von Unbefugten weder errechnet, noch erraten werden können. Allgemein bieten kürzere Schlüssel einen schlechteren Schutz als längere [MOV96, S. 21], jedoch darf nicht davon ausgegangen werden, dass ein Verfahren sicher ist, nur weil es komplexe Schlüssel verwendet. Spezielle mathematische Verfahren können mit kürzeren Schlüsseln ein ähnliches Sicherheitsniveau erreichen wie andere Verfahren mit deut-

[2] Der Beweis gelang bisher nur bei dem Vernam-Verfahren. Bei diesem symmetrischen Verfahren muss der Schlüssel mindestens so viele Zeichen umfassen, wie der zu verschlüsselnde Text. Der Schlüssel darf auch nur ein einziges Mal verwendet werden und muss absolut zufällig sein. Vgl. [MOV96, S. 21], [Mil03, S. 84ff].

lich längeren Schlüsseln [Sch01a, S. 93]. Aktuelle Anwendungen verwenden als Schlüssel Zeichen- oder Zahlenfolgen, die einige hundert bis mehrere tausend Stellen umfassen.

Verschlüsselte Nachrichten können über unsichere Kanäle übermittelt werden, ohne *Vertraulichkeit* und *Integrität* der Nachrichten zu gefährden [MOV96, S. 4]. Sofern der verwendete Schlüssel eindeutig einem Absender zugeordnet werden kann, dient die Verschlüsselung dem Empfänger ferner zur *Identifikation* und *Authentifikation* des Absenders. Um die *Urheberschaft* der Nachricht zweifelsfrei beweisen zu können, darf auch der Empfänger keine Kenntnis des Absenderschlüssels haben.

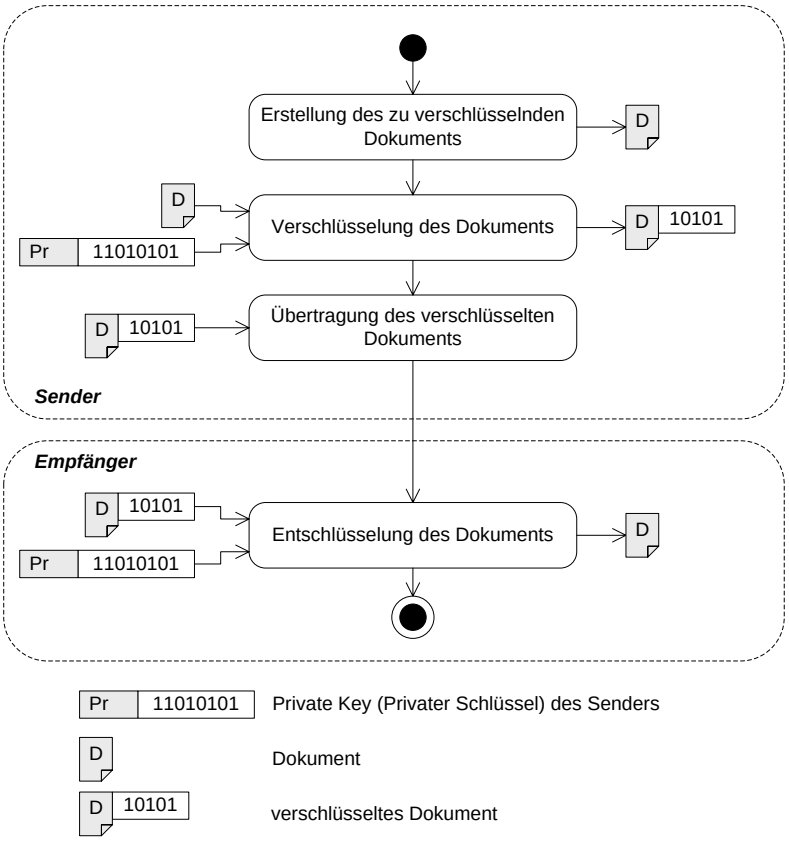

Abbildung 2: Ablauf der symmetrischen Ver- und Entschlüsselung

Symmetrische Verschlüsselung

In Abbildung 3.1.1 ist *Symmetrische Verschlüsselung* schematisch dargestellt. Dieser Vorgang zeichnet sich dadurch aus, dass zum Ver- und Entschlüsseln jeweils derselbe Schlüssel erforderlich ist. Das ist für bilaterale Kommunikation

gewöhnlich nicht hinderlich, birgt aber gewisse Einschränkungen, sofern mehr als zwei Parteien beteiligt sind. Die Urheberschaft kann nicht eindeutig nachgewiesen werden, da alle legitimen Empfänger auch Sender sein können. Der tatsächliche Sender kann seine Urheberschaft leugnen (*Nichtanerkennung*), andere können sie für sich beanspruchen. Die Kommunikationspartner müssen sich außerdem vor Beginn der eigentlichen Kommunikation auf einen gemeinsamen Schlüssel einigen. Dafür benötigen sie bereits einen geschützten Kanal. Für eine Signatur sind solche Verfahren nur eingeschränkt geeignet.

Asymmetrische Verschlüsselung

Durch die Entwicklung *asymmetrischer Verschlüsselungsverfahren* wurde versucht, diesen Hindernissen zu begegnen. Dabei kommt ein Schlüsselpaar, bestehend aus einem *öffentlichen* und einem *privaten Schlüssel*, zum Einsatz. Mit dem öffentlichen Schlüssel können Nachrichten verschlüsselt werden, so dass nur der Inhaber des privaten Schlüssels sie wieder entschlüsseln kann. Mit dem privaten Schlüssel können Signaturen erzeugt werden, die wiederum von allen Inhabern des öffentlichen Schlüssels geprüft werden können. Der öffentliche Schlüssel kann über unsichere Kanäle publiziert werden, ohne die Sicherheit einzuschränken. Bei Verwendung eines symmetrischen Verfahrens wird mindestens einen Schlüssel pro Kommunikationspfad benötigt. Kommunizieren beispielsweise sechs Personen miteinander, so existieren bereits 15 mögliche Kommunikationspfade, es werden also 15 symmetrische Schlüssel benötigt ($\binom{n}{2}$ Schlüssel für n Personen). Dagegen genügt bei asymmetrischen Verfahren ein Schlüsselpaar je Kommunikationsendpunkt – also sechs Schlüsselpaare für sechs Personen. Da nur der Inhaber des privaten Schlüssels signieren kann, sind asymmetrische Verfahren gut zur Identifikation, Authentifikation und zum Urheberschaftsnachweis geeignet [Eck04, S. 374].

Um eine Nachricht zu signieren, könnte sie vollständig mit dem privaten Schlüssel verschlüsselt werden. Jeder, der über das öffentliche Gegenstück verfügt, könnte so eine Nachricht wieder entschlüsseln. Wenn das gelingt, sind Herkunft und Unversehrtheit der Nachricht sichergestellt. Wenn die Nachricht manipuliert worden wäre oder nicht vom angegebenen Absender stammen würde, so ließe sie sich nicht fehlerfrei entschlüsseln. Diese Variante hat allerdings wieder einige Nachteile, so dass noch ein weiterer Schritt notwendig wird, der Einsatz von so genannten Hashverfahren.

3.1.2 Hashverfahren

Als Signatur ein mit einem privaten Schlüssel vollständig verschlüsseltes Dokument zu verwenden ist aus mehreren Gründen nicht sinnvoll. Eine solche Signatur ist mindestens so umfangreich wie das ursprüngliche Dokument. Wenn sie zusammen mit dem Dokument verschickt oder archiviert werden soll, verdoppelt sich der Speicherbedarf. Wird stattdessen nur das verschlüsselte Dokument verschickt oder gespeichert, ist es ohne den öffentlichen Schlüssel nicht zu lesen. Geht der Schlüssel verloren, ist die Nachricht ebenso verloren.

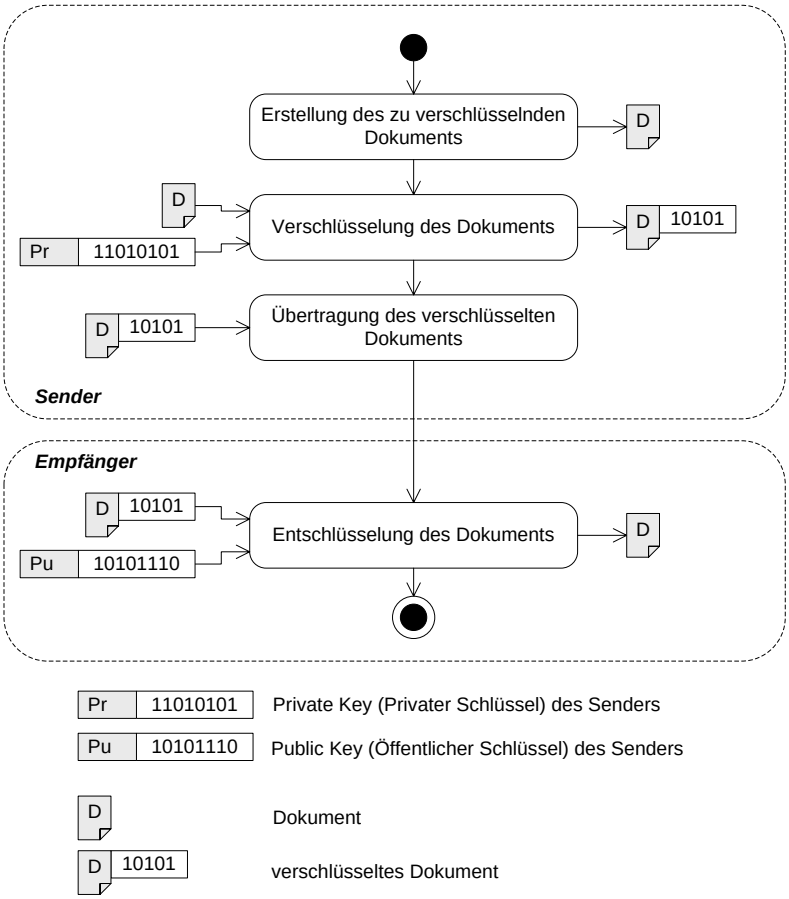

Abbildung 3: Ablauf der asymmetrischen Ver- und Entschlüsselung

Wenn eine Nachricht mehrere Signaturen erfordert, so vervielfacht sich entweder der Speicherbedarf oder der Text wird mehrfach verschlüsselt. Dabei können sich die Verfasser der nachfolgenden Signaturen nie ganz sicher sein, was sie eigentlich signieren. Soll das Dokument später geprüft oder gelesen werden, müssen alle Signaturen in einer festen Reihenfolge entfernt werden. Fehlt nur ein einziger Schlüssel, so ist das Dokument nicht lesbar. Weiterhin sind asymmetrische Verschlüsselungsverfahren sehr rechenintensiv. Der Aufwand steigt dabei mit der Länge des zu signierenden Dokumentes. Das gilt sowohl für das Ver- als auch für das Entschlüsseln und besonders für mehrfach verschlüsselte Dokumente. Schließlich existieren in einigen Ländern strenge gesetzliche Restriktionen in Bezug auf die Nutzung von Kryptographie zur Verschlüsselung [Eck04, S. 347ff].

Einwegfunktionen

Statt einer Verschlüsselung des gesamten Dokumentes wird zum Zweck einer Signatur meist nur eine Prüfsumme des Dokumentes berechnet und verschlüsselt. Diese *Prüfsummen* werden mit sogenannten *Einwegfunktionen* berechnet. „Eine Einwegfunktion ist eine Funktion, die einfach auszuführen, aber schwer – praktisch unmöglich – zu invertieren [umzukehren] ist“ [BSW04, S. 12]. Ein einfaches Beispiel für eine Einwegfunktion ist die Quersumme, das ist die Summe aller einzelnen Ziffern einer Zahl. Die Quersumme von 23 ist beispielsweise $\mathrm{Q}(23) = 2 + 3 = 5$. Eine Umkehrfunktion (*Inversion*) für diese Funktion existiert nicht, für eine gegebene Quersumme kann nicht festgestellt werden, aus welcher Zahl sie ursprünglich berechnet wurde: Die Quersumme 5 kann aus $14, 41, 401, 1004, 23, 32, 3020, 5000$ und unendlich vielen weiteren Zahlen berechnet werden.

Kollisionsfreiheit

Nun kann es passieren, dass die Prüfsummenberechnung für zwei unterschiedliche Dokumente zu dem selben Ergebnis führt – so wie in dem Beispiel mit der Quersumme. Dieses Phänomen wird als *Kollision* bezeichnet. Tritt eine solche Kollision auf, so sind nicht nur die Prüfsummen der Dokumente, sondern auch alle Signaturen, die mit der Prüfsumme erstellt werden, gleich. Ein Angreifer kann unbemerkt ein signiertes Dokument durch ein anderes, mit der gleichen Prüfsumme aber anderem Inhalt, austauschen. Um diese Situation zu vermeiden werden *kollisionsfreie* Einwegfunktionen eingesetzt, bei denen es extrem unwahrscheinlich ist, zwei unterschiedliche Dokumente mit derselben Prüfsumme zu finden. Aus praktischen Gründen werden bevorzugt Funktionen verwendet, deren Ergebnis eine feste Länge hat, unabhängig vom Umfang des Eingabetextes. Funktionen, die diese Eigenschaften erfüllen, heißen *Hashfunktionen*, ihr Ergebnis *Hashwert* oder einfach Hash [BSW04, S. 13].

Hashwerte in Signaturen

Durch die Verschlüsselung der Hashwerte anstelle des gesamten Dokumentes werden viele Probleme gelöst: Die Berechnung der Hashwerte ist auch für umfangreiche Dokumente schnell durchführbar, die Ver- und Entschlüsselung der im Vergleich zum Dokument sehr kurzen Hashwerte ebenso. Der Speicherbedarf der Signatur ist gering, das Dokument bleibt dennoch jederzeit auch ohne Schlüssel lesbar und es kann schnell durchsucht werden. Mehrere Signaturen können problemlos zu einem Dokument hinzugefügt werden. Spätere Signaturen können bereits vorhandene mit einschließen (z. B. bei Beglaubigungen). Neue Signaturen können auch nur das eigentliche Dokument betreffen und unabhängig neben bereits vorhandenen Signaturen stehen. Alle Signaturen können unabhängig voneinander geprüft werden. Es ist sogar möglich, Signaturen vom Dokument getrennt aufzubewahren, beispielsweise um den Speicherbedarf einer operativ genutzten Datenbank gering zu halten. Schließlich gelten für das Signieren, also das Verschlüsseln von Hashwerten, in einigen Ländern andere Gesetze als für das Verschlüsseln von ganzen Dokumenten. So schränkt zum Beispiel das Wassenaar-Abkommen, das zwischen 33 Industrienationen (darunter Deutschland) abgeschlossen wurde, den Export von kryptografischen Produkten ein. Produkte zur elektronischen Si-

gnierung sind ausdrücklich ausgenommen, für sie gelten die Einschränkungen nicht [Eck04, S. 350].

3.1.3 Elektronisch signierte Zeitstempel

In bestimmten Situationen ist es notwendig, nachzuweisen, dass eine bestimmte Information zu einem bestimmten Zeitpunkt vorlag. Zum Beispiel um zu zeigen, dass eine bestimmte Erfindung bereits genutzt wurde, bevor ein anderer sie zum Patent eingereicht hat oder, dass eine vertraglich vereinbarte Leistung fristgerecht erbracht wurde. In derartigen Situationen ist es möglich, einen elektronisch signierten *Zeitstempel* einzusetzen. Dafür genügt es, das Dokument mit dem aktuellen Datum und der aktuellen Uhrzeit zu versehen und anschließend elektronisch zu signieren. Im Grunde entspricht der Vorgang der weit verbreiteten Praxis, vor eine manuelle Unterschrift das aktuelle Datum zu setzen. Der ebenfalls verbreitete Brauch, auch den Ort der Unterschrift anzugeben, hat bisher keine analoge Entsprechung bei elektronischen Signaturen gefunden, ist aber genauso möglich, falls ein bestimmter Einsatzzweck es erfordert.

Vertrauen steigern

Technisch kann nicht verhindert werden, dass dabei ein falsches Datum signiert wird. Um einen dahingehenden Verdacht auszuräumen bietet es sich an, die Signatur durch eine Person vornehmen zu lassen, die das Vertrauen aller Adressaten des fraglichen Dokumentes genießt. Dafür existieren spezielle *Zeitstempeldienstanbieter*. Weiterhin wurden verschiedene Mechanismen entwickelt, die einen Betrug mit falschen Zeitstempeln noch weiter erschweren. Dazu können in einen aktuellen Zeitstempel Angaben zu den zuvor signierten Dokumenten gemacht werden [Sch96, S. 76ff]. Damit ist die Reihenfolge, in der die Signaturen getätigt wurden, festgehalten. Die Inhaber der später signierten Dokumente können als Zeugen für die früher signierten auftreten. Denkbar wäre auch die Veröffentlichung von Zeitstempeln in Tageszeitungen oder ähnliches.

Vertraulichkeit bewahren

Gerade die letzten beiden Vorschläge zeigen, dass es nicht immer sinnvoll ist, dem Zeitstempeldienstanbieter das zu beglaubigende Dokument vollständig zur Verfügung zu stellen. Es genügt jedoch vollkommen, einen Hashwert über das Dokument zu bilden und diesen mit einem Zeitstempel versehen zu lassen. So können auch streng geheime Dokumente problemlos mit einem Zeitstempel versehen werden, und der Zeitstempel kann beliebig veröffentlicht werden, da der Hashwert keinen Rückschluss auf den Inhalt des Dokumentes zulässt. Weiterhin hat dieses Verfahren bei umfangreichen Dokumenten auch Performance Vorteile, da nicht das ganze Dokument, sondern nur der wesentlich kürzere Hashwert zwischen Dokumentinhaber und Zeitstempeldienstanbieter ausgetauscht werden muss.