Digitale Signaturen

Die digitale Signatur gewinnt auf Grund der zunehmenden elektronische Austausch von Dokumenten immer mehr an Bedeutung. Diese Ausarbeitung befasst sich im Rahmen der Vorlesung „Communication Technologies I“ mit den Verfahren und Aufgaben der digitalen Signaturen.

Ein Referat von

Jan Bader	20019259
Andreas Pirali	20010148
Marc Selig	20002693

Inhalt

1 Einleitung

In Zeiten, in denen es üblich geworden ist, Dokumente auf elektronischem Weg per E-Mail, über das Internet oder in lokalen Netzwerken zu versenden, war es unbedingt nötig zu klären, wie die handschriftliche Unterschrift adäquat zu ersetzen ist.
Ob beim Informationsaustausch mit Behörden, Banken oder Geschäftspartnern, der Kommunikation hoch sensibler medizinischer Daten, vertraulicher Dokumente oder Zahlungsanweisungen - eine eindeutige Identifizierbarkeit des Absenders ist auf vielen Feldern als höchst wichtig einzustufen.
Man denke in diesem Zusammenhang nur daran, wo überall im täglichen Leben Unterschriften getätigt werden. Die Notwendigkeit eines Ersatz' auf elektronischer Basis wird dabei leicht ersichtlich.

2 Was digitale Signaturen sind

Bei digitalen Signaturen handelt es sich um elektronische Daten, die die eindeutige Identifizierung des Verfassers zur Erklärung des Willens oder zur Bestätigung von Vorgängen ermöglichen. Mit diesem Ziel nicht zu verwechseln ist die Integrität des Dokuments, die Auskunft darüber gibt, ob das Dokument verändert wurde, seitdem der Verfasser das Dokument geschlossen hat.
Es ist also zu Unterscheiden zwischen Authentizität und Integrität.
Oft werden Verschlüsselung des Dokuments und Integrität mit zur digitalen Signatur hinzugerechnet, was aber nicht in jedem Fall richtig ist. Die digitale Signatur verwendet oft Werkzeuge, die auch diese Funktionen zulassen, die Hauptaufgabe ist allerdings das Möglich machen der eindeutigen Bestimmung des Verfassers. Dies geschieht meist über Zertifikate oder über bei der Signaturerstellung biometrisch erfasste eigenhändige Unterschriften.
Weiterhin ist es wichtig, zwischen den Begriffen Authentisierung und Autorisierung zu unterscheiden. Authentisierung bedeutet die Überprüfung einer Identität, während Autorisierung das Verleihen bestimmter Rechte und Zuständigkeiten beschreibt. Bei der normalen Unterschrift, mit der im täglichen Leben Schriftstücke unterzeichnet werden, wird bisweilen beides abgehandelt.

An dieser Stelle soll auch angemerkt werden, dass der Begriff „Digitale Signatur“ in der aktuellen Gesetzgebung nicht mehr verwendet wird, sondern durch „Elektronische Signatur“ ersetzt wurde.

3 Unterschiede digitaler Signaturen

Es gibt drei Arten von digitalen Signaturen:

3.1 Einfache Signaturen

Unter einfachen Signaturen versteht das Signaturgesetz (§2 Nr.1 SigG) Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentisierung dienen.
Beispiele dafür sind elektronische Visitenkarten oder eingescannte Unterschriften.

3.2 Fortgeschrittene Signaturen

Als fortgeschrittene Signaturen beschreibt das Signaturgesetz (§2 Nr.2 SigG) elektronische Signaturen nach Punkt 1.1, die

1. ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
2. die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
3. die mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
4. mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Beispiele: Signaturen im Rahmen von Pretty Good Privacy (PGP), Softwarezertifikate

3.3 Qualifizierte Signaturen

Fortgeschrittene elektronische Signaturen sind nach §2 Nr. 2 SigG Signaturen nach Punkt 1.2, die

1. auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
2. mit einer sicheren Signaturerstellungseinheit erzeugt werden.

Beispiel: Signaturen auf elektronischen Signaturkarten, soweit sie von Zertifizierungsdienstanbietern erzeugt wurden, die sich nach dem SigG angezeigt haben.

3.4 Signaturen als Beweismittel vor Gericht

Dieses Thema ist sehr komplex, deswegen soll hier nur eine kleine Randbemerkung darauf hinweisen, dass entgegen der landläufigen Meinung auch nichtqualifizierte Signaturen vor Gericht verwendet werden können.
Entscheidend in einem Zivilprozess ist die Beweisbarkeit einer Willenserklärung. Diese Beweisbarkeit kann möglicherweise auch durch ein nichtqualifiziertes Signaturverfahren nachgewiesen werden. Eine qualifizierte Signatur ist nur dann erforderlich, wenn dies explizit durch ein Gesetz vorgeschrieben ist.

4 Beispiele für digitale Signaturen

Wenn persönliche Willenserklärungen abgegeben werden, muss jedes Dokument mit einer individuell erstellten digitalen Signatur versehen werden.
Oft reichen einfache oder fortgeschrittene Signaturverfahren aus, die qualifizierte Signatur ist nur selten erforderlich. Dies erspart der signierenden Person Kosten und Aufwand.
Bei Paketzustellungen ist es beispielsweise so, dass die Identifizierung der Person durch den Paketboten erfolgt. Wird also die Unterschrift auf ein Unterschriftentablett abgegeben, so kann in diesem Fall auf ein zusätzliches Zertifikat verzichtet werden, da erst bei Bedarf die beweisrelevante Identifizierung durch einen Schriftsachverständigen durchgeführt wird.

Anders verhält es sich bei im Internet aufgegebenen Bestellungen. Hier ist eine Identifizierung des Auftraggebers schon im Moment der Auftragsabgabe wünschenswert. Da bietet sich die Identifizierung durch eine zertifizierte qualifizierte Signatur an, die eben dieses ermöglicht.

5 Ein kurzes Wort zur Biometrie

Bei fortgeschrittenen und qualifizierten Signaturen ist gesetzlich vorgeschrieben, dass der Inhaber der Signatur die alleinige Kontrolle über das Hinzufügen einer Signatur hat.
Bei asymmetrischen Verfahren mit Public- und Private-Key wird zur Sicherstellung, dass nur der Eigentümer des Private-Key diesen benutzen kann, heutzutage häufig

ein Pin-Verfahren angewendet. Also kann nur derjenige, der Kenntnis vom Pin-Code hat, kann auch mit dem Private-Key ein Dokument signieren.
Beispiel (qualifizierte Signatur):
Der Private-Key ist auf einer Chip-Karte gespeichert. Die Chip-Karte wird über ein Kartenlesegerät ausgelesen, welches mit einem Pin-Code freigeschaltet werden muss.
Da in den letzten Jahren die Erkenntnisse und technischen Möglichkeiten zur Erfassung biometrischer Daten so weit zugenommen haben, dass einem praktischen Einsatz dieses Verfahrens als Ersatz für den Pin-Code nichts mehr im Wege steht, darf auch der Frage nachgegangen werden (allerdings nicht an dieser Stelle), warum diese Technik nicht schon viel häufiger eingesetzt wird.
Bei biometrischen Merkmalen muss man zwischen passiven biometrischen Erkennungsmerkmalen wie Fingerabdruck und Iriserkennung und aktiven Erkennungsmerkmalen wie Spracherkennung und Unterschrift unterscheiden.
Die Unterschrift gilt zusätzlich als Lebenderkennung und enthält eine Warn- und Schutzfunktion, da sie niemals ungewollt abgegeben werden kann.

Aber auch bei einfachen oder fortgeschrittenen Signaturen können biometrische Erkennungsmerkmale - insbesondere die Unterschrift - zum Einsatz kommen.
So ist vorstellbar, dass eine gescannte Unterschrift einem Dokument hinzugefügt wird und unter Einbeziehung dieses Bildes aus dem Dokument ein Hashwert errechnet wird.
Denkbar ist beispielsweise ein Verfahren, bei dem eine Person bei einem Anbieter eine Vergleichsunterschrift hinterlegt. Soll nun einem Dokument eine Signatur in Form einer Unterschrift hinzugefügt werden, wird die hinzugefügte Signatur mit der bei dem Anbieter hinterlegten Signatur verglichen und so festgestellt, ob es sich wirklich um den „Eigentümer“ der Unterschrift handelt.
Dies ist ein vorbeugender Schutz, haftungsrelevant ist allerdings die Unterschrift, die dem Dokument hinzugefügt wurde und die von forensischen Spezialisten wie Schriftsachverständigen eindeutig zugeordnet werden kann.

6 Methoden der Verschlüsselung

Um „Digitale Signaturen“ zu ermöglichen, werden verschiedene Verfahren der Verschlüsselung angewandt.

6.1 Ein-Weg-Verschlüsselung

Bei der Einwegverschlüsselung handelt es sich um ein Verfahren, Daten so zu verschlüsseln, dass sie nicht mehr entschlüsselt werden können. Daher auch der Begriff „Ein-Weg-Verschlüsselung“.
Praktisch angewandt wird dies zum Beispiel, um die Unverfälschtheit eines Dokuments zu überprüfen.
Der Verfasser lässt dazu eine Prüfsumme (Hashwert) aus einem Dokument errechnen. Die Prüfsumme muss so angelegt sein, dass eine Rekonstruktion des Dokuments daraus unmöglich ist. Es handelt sich also um eine Ein-Weg-Verschlüsselung. Außerdem soll es unmöglich sein, einen Text zu erstellen, der die selbe Prüfsumme hervorbringt.
Dann werden Dokument und Prüfsumme auf unterschiedlichen Wegen unabhängig voneinander übermittelt. Wenn der Empfänger ebenfalls die Prüfsumme aus dem Dokument errechnen lässt und die beiden Prüfsummen übereinstimmen, wurde das Dokument nicht verändert.
Der Nachteil dieses Verfahrens ist, dass zwei unterschiedliche Kommunikationswege gefunden werden müssen: einer für das Dokument und einer für die Prüfsumme.
Die Lösung, um diesen Nachteil aufzuheben, ist eine weitere Verschlüsselung, wie weiter unten gezeigt werden wird.

6.2 Symmetrische Verschlüsselung

Die einfachste Art ein Dokument zu verschlüsseln und wieder zu entschlüsseln stellt die symmetrische Verschlüsselung dar. Um was es sich dabei handelt, soll kurz an einem sehr einfachen Beispiel erklärt werden:

1. Man nimmt den Text „Dies ist ein Text“ und tauscht die Buchstaben jeweils gegen die im Alphabet nächsten aus.
   „Dies ist ein Text“ wird also zu „Ejft jtu fjo Ufyu“.
2. Diese Botschaft wird an den Empfänger übermittelt.
3. Der Schlüssel wird ebenfalls an den Empfänger übermittelt, denn um den Text zu entschlüsseln, benötigt der Empfänger ebenfalls den Schlüssel, der in diesem Fall lauten würde: „Buchstabe wurde durch den nächsten im Alphabet ersetzt.“ ($B_2 = B_1 + 1$)
4. Mit diesem Schlüssel kann dann wieder der ursprüngliche Text rekonstruiert werden. ($B_1 = B_2 – 1$) (Wobei in diesem einfachen Beispiel der Schlüssel na-

türlich auch durch andere Verfahren gefunden werden kann, er also sehr unsicher ist.)

Da sowohl Versender als auch Empfänger denselben Schlüssel verwenden, wird dieses Verfahren als symmetrische Verschlüsselung bezeichnet.

Nachteil dieses Verfahrens ist, dass der Schlüssel an den Empfänger übermittelt werden muss. Und wenn der Schlüssel abgefangen wird, kann nicht mehr festgestellt werden, ob der Text verändert wurde und von wem der Text stammt.

Der Vorteil gegenüber der asymmetrischen Verschlüsselung, die als nächstes erklärt wird, ist die Geschwindigkeit, mit der eine Ver- bzw. Entschlüsselung stattfinden kann. Diese ist wesentlich höher als bei der aufwendigen asymmetrischen Ver- und Entschlüsselung.

6.3 Asymmetrische Verschlüsselung

Bei asymmetrischer Verschlüsselung verwenden Versender und Empfänger unterschiedliche Schlüssel, die jeweils nur Ver- oder Entschlüsselung zulassen. Aus dem Schlüssel zur Verschlüsselung lässt sich der Schlüssel zur Entschlüsselung nicht gewinnen. Ebenso ist der umgekehrte Weg versperrt, also die Gewinnung des Schlüssels zur Verschlüsselung aus dem Schlüssel zur Entschlüsselung.
Weil bei diesem Verfahren zwei unterschiedliche Schlüssel verwendet werden, spricht man von asymmetrischer Verschlüsselung.
Dieses Verfahren ist üblich, um aus Prüfsummen durch eine sichere Übermittlung digitale Signaturen zu machen.

Für dieses Verfahren ist ein Private-Key nötig, der nur dem Eigentümer zugänglich ist. Meist wird solch ein Key auf einer Chip-Karte gespeichert und über ein Kartenlesegerät eingelesen, um ihn dann auf ein Dokument anzuwenden.
Des Weiteren ist ein Public-Key notwendig, der bei einer Zertifizierungsstelle hinterlegt ist und dort von jedermann abgerufen werden kann.
Durch diese Zertifizierungsstelle ist auch die Identität des Eigentümers eindeutig bestimmt, so dass sich aufgrund des öffentlichen Schlüssels der Absender des Dokuments eindeutig feststellen lässt.

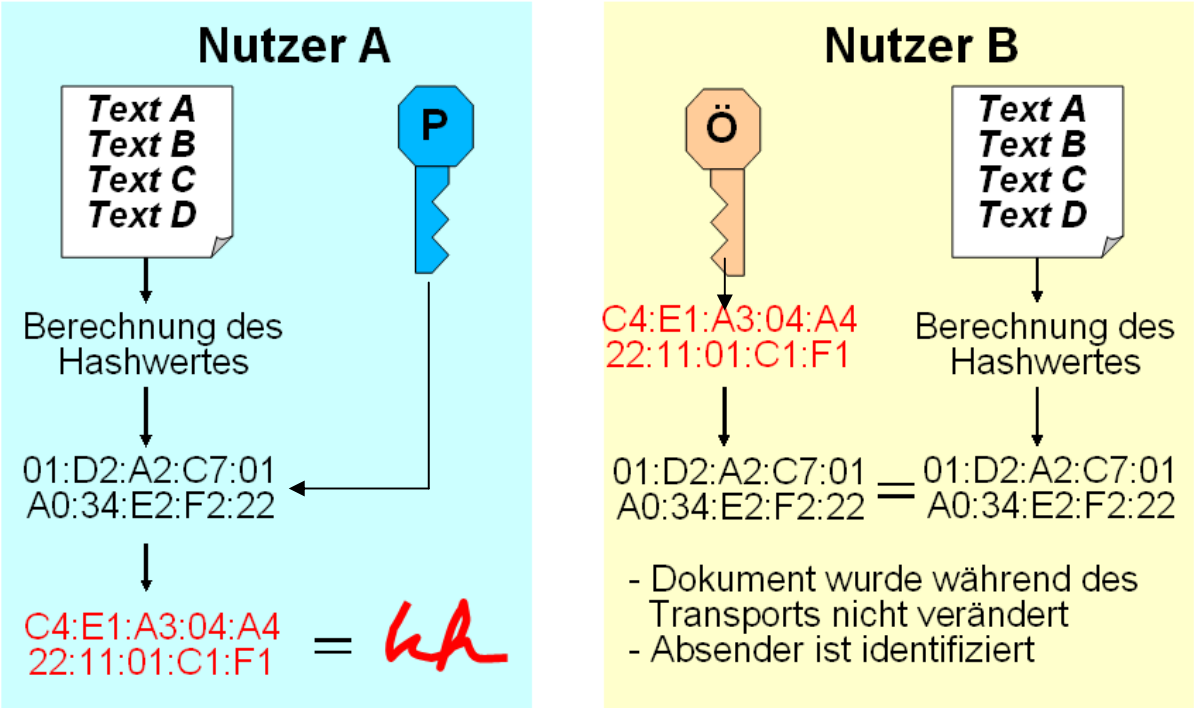

Abbildung 6.1: Erstellung und Prüfung einer digitalen Signatur

Abbildung 6.1 zeigt, wie die Ein-Weg-Verschlüsselung und die asymmetrische Verschlüsselung kombiniert werden, um die Ziele der digitalen Signatur zu erreichen.

1. Nutzer A berechnet die Prüfsumme des zu signierenden Dokuments (Ein-Weg-Verschlüsselung)
2. Diese Prüfsumme wird mit dem Private-Key verschlüsselt. Diese Daten werden zur digitalen Signatur.
3. Sowohl die digitale Signatur als auch das Dokument werden an Nutzer B übermittelt.
4. Nutzer B wendet den Public-Key auf die verschlüsselte Prüfsumme an und erhält damit die unverschlüsselte Prüfsumme des ursprünglichen Dokuments.
5. Außerdem berechnet er aus dem Dokument die Prüfsumme.
6. Wenn diese beiden Prüfsummen übereinstimmen, steht eindeutig fest, dass das Dokument seid der Verschlüsselung mit dem Private-Key nicht verändert wurde.
7. Dadurch, dass nur einer Person der Private-Key bekannt ist, ist somit auch bekannt, wer das Dokument signiert hat.

Private- und Public-Key lassen noch eine zusätzliche Funktion zu, die aber nicht das primäre Ziel der digitalen Signatur verfolgt, nämlich das Verschlüsseln eines Dokuments.

Durch Anwenden des Public-Keys auf ein Dokument wird ein Dokument verschlüsselt. Diese Verschlüsselung kann nur durch das Anwenden des Private-Keys auf das verschlüsselte Dokument wieder aufgehoben werden.

6.4 Hybride Verfahren

Der Nachteil der asymmetrischen Verschlüsselung gegenüber der symmetrischen Verschlüsselung ist der höhere Aufwand zur Ver- und Entschlüsselung.
Aus diesem Grund werden in der Praxis häufig Verfahren eingesetzt, in denen diese beiden Methoden kombiniert werden.

Ein Beispiel:

1. Ein symmetrischer Schlüssel wird für einmaligen Gebrauch zufällig generiert.
2. Dieser wird auf ein Dokument angewendet.
3. Auf diesen symmetrischen Schlüssel wird der Public-Key des Empfängers angewendet und so der symmetrische Schlüssel verschlüsselt.
4. Dieser asymmetrisch verschlüsselte symmetrische Schlüssel wird zusätzlich zu dem Dokument übertragen.
5. Der Empfänger entschlüsselt mit dem Private-Key den symmetrischen Schlüssel.
6. Dieser wird dann auf das Dokument angewendet, das somit wieder lesbar wird.

Da in diesem Fall nur der symmetrische Schlüssel asymmetrisch verschlüsselt wird, bleibt der Aufwand relativ gering. Der große Schwachpunkt bei symmetrischen Schlüsseln, die Übertragung, wird mit diesem Verfahren sicher gemacht und somit kombiniert diese Methode hohe Geschwindigkeit mit großer Sicherheit.

Ein anderes Beispiel ist das SSL-Verfahren, welches ebenfalls die Vorteile beider Verschlüsselungstechniken kombiniert.

7 Beispiel RSA

Bei RSA handelt es sich um ein asymmetrisches Verschlüsselungsverfahren, welches meistens bei der Verschlüsselung von E-Mails eingesetzt wird. Asymmetrische Verschlüsselungsverfahren beruhen darauf, dass man Produkte aus zwei großen Primzahlen nur mit sehr großem Rechenaufwand wieder in die beiden Primzahlen zerlegen kann.
Man wählt bei RSA zwei zufällige Primzahlen *p* und *q*. Bei einer 1024Bit-Verschlüsselung liegen diese Zahlen in der Größenordnung von 10^{150}. Aus diesen beiden Zahlen bildet man das Produkt $n = p*q$. *n* ist Bestandteil sowohl des öffentlichen wie auch des privaten Schlüssels und liegt in der Größenordnung 10^{300}.
Von diesem Produkt *n* muss nun die Eulersche Phi-Funktion $\Phi(n)$ bestimmt werden. Die Eulersche Phi-Funktion sagt aus, wie viele Zahlen, die kleiner als *n* sind, teilerfremd zu *n*, also kein Teiler von *n*, sind. Um die Phi-Funktion auszurechnen müssen sämtliche Zahlen, die kleiner als *n* sind, in ihre Primfaktoren zerlegt werden. Diese Primfaktoren einer Zahl müssen alle unterschiedlich zu den Primfaktoren von *n* sein. Dann ist diese Zahl teilerfremd zu *n*. Die Anzahl der teilerfremden Zahlen ergibt die Phi-Funktion. Wie hieraus ersichtlich, ist die Berechnung der Eulerschen Phi-Funktion sehr aufwendig. Für Primzahlen gibt es jedoch eine wesentliche Vereinfachung. Primzahlen sind nur durch sich selbst und durch eins teilbar, also sind alle Zahlen kleiner *n* außer 1 teilerfremd. Man kann also für Primzahlen schreiben: $\Phi(p) = p-1$. Des Weiteren gilt, dass die Phi-Funktion eines Produktes das Produkt der Phi-Funktionen der einzelnen Faktoren ist, also $\Phi(p*q) = \Phi(p) * \Phi(q)$. Für zwei Primzahlen kann man nun einfach schreiben:

$$\Phi(p*q) = (p-1) * (q-1)$$

Somit kann man auch leicht die Phi-Funktion von *n*, also dem Produkt aus *p* und *q,* ausrechnen:

$$\Phi(n) = (p-1) * (q-1)$$

Nun wählt man zufällig eine Zahl *e*, die lediglich teilerfremd zu $\Phi(n)$ sein muss. Die Zahlen *e* und *n* bilden den öffentlichen Schlüssel.
Den privaten Schlüssel *d* erhält man nun durch folgende Modulo-Operation:

$$e * d \,\%\, \Phi(n) = 1$$

Dies bedeutet, dass das Produkt *e*d* bei der Division durch *Φ(n)* den Rest 1 aufweisen muss. Durch den Euklidschen Algorithmus erhält man folgenden Ausdruck zur Bestimmung von *d*:

$$e * d = k * \Phi(n) + 1$$

$$d = (k * \Phi(n) + 1) / e$$

Aus dieser Gleichung bestimmt man für eine willkürliche ganze Zahl *k* ein ganzzahliges *d*. Hieraus ist ersichtlich, dass verschiedene *d* als Lösung der Gleichung möglich sind. Somit gibt es auch mehrere private Schlüssel zu einem gewählten öffentlichen Schlüssel *e*. Dies ist jedoch eher unkritisch einzustufen, da die ganzzahligen Lösungen für *d* immer den Abstand *Φ(n)* zu einander haben. In der Praxis liegt *Φ(n)* in der Größenordnung von 10^{300}, so dass der Abstand zwischen den möglichen Lösungen sehr groß ist und die Anzahl in Abhängigkeit von dem zur Verfügung stehenden Zahlenbereich sehr gering wird. Die Zahlen *d* und *n* bilden nun den privaten Schlüssel.
Zum Verschlüsseln einer Nachricht muss folgende Operation durchgeführt werden: Die zu verschlüsselnde Zahl muss zunächst mit der Zahl *e* des öffentlichen Schlüssels potenziert werden und anschließend mit der Modulo-Operation mit *n* verknüpft werden, also:

$$Geheimzahl = (Klartext)^e \ \% \ n$$

Zur Entschlüsselung muss die Geheimzahl vor der Modulo-Operation anstatt mit *e* mit *d* potenziert werden:

$$Klartext = (Geheimzahl)^d \ \% \ n$$

Ein konkretes Zahlenbeispiel soll die Schlüsselerzeugung und die Ver- und Entschlüsselung verdeutlichen. Wir wählen als Primzahlen *p = 3* und *q = 7*. Daraus folgt für *n = p * q = 3 * 7 = 21*. Die Eulersche Phi-Funktion von 21 bestimmen wir auf folgende Weise: *Φ(n) = Φ(p*q) = Φ(p) * Φ(q) = (p-1) * (q-1) = 2 * 6 = 12*. Für *e* wählen wir die Zahl 11, die teilerfremd zu *Φ(n)* ist.
Den privaten Schlüssel *d* bestimmen wir nun über die Gleichung

$$e * d = k * \Phi(n) + 1$$

$$11 * d = k * 12 + 1$$

Für $k = 10$ erhalten wir für d die ganzzahlige Lösung 11, da aber in diesem Falle $e = d$ wäre, verwerfen wir diese Lösung. Für $k = 21$ ergibt sich $d = 23$.
Den öffentlichen Schlüssel bilden somit $e = 11$ und $n = 21$, den privaten $d = 23$ und $n = 21$.
Wir wollen nun die Zahl 9 mit dem öffentlichen Schlüssel verschlüsseln:

$$Geheimzahl = (Klartext)^{e} \% n$$

$$Geheimzahl = (9)^{11} \% 21$$

$$Geheimzahl = 31381059609 \% 21$$

$$Geheimzahl = 18$$

Die Zahl 18 würde nun übertragen. Der Besitzer des privaten Schlüssels kann diese folgendermaßen wieder entschlüsseln:

$$Klartext = (Geheimzahl)^{d} \% n$$

$$Klartext = (18)^{23} \% 21$$

$$Klartext = 743477136140219279133187768 32 \% 21$$

$$Klartext = 9$$

Aus diesem kleinen Beispiel wurde deutlich, wie der RSA-Algorithmus funktioniert. Es wurde aber auch deutlich, wie rechenaufwendig eine asymmetrische Verschlüsselung ist. Bei zweistelligen Schlüsseln bildeten sich in unserem Beispiel schon 29-stellige Zwischenergebnisse.

8 Schlüssellängen für die Erstellung digitaler Signaturen

Für die Erstellung von digitalen Signaturen werden so genannte Hashfunktionen verwendet, an die spezielle Anforderungen gestellt werden müssen, um sicherzustellen, dass diese nicht „geknackt“ werden können. Die Hashfunktion muss folgende Anforderungen erfüllen:

1 Die Funktion muss **kollisionresistent** sein, was bedeutet, dass es unmöglich sein muss 2 verschiedene Texte mit demselben Hashwert zu erzeugen.

2 Es muss sich um eine **Einweg**-Funktion handeln, das heißt es muss un möglich sein, aus einem bekannten Hashwert den zugehörigen Text zu generieren.

Von der in Deutschland zuständigen Behörde, der Regulierungsbehörde für Telekommunikation und Post (RegTP), werden zwei Verfahren zur Erzeugung der Hashwerte vorgeschlagen. Die vorgeschlagenen Verfahren sind das SHA-1 und das RIPEMD-160. Beide erzeugen aus einem Text beliebiger Länge eine 160 Bit-langen Hashwert. Diese Verfahren sollen bis Ende 2010 sicher sein, soweit das heute gesagt werden kann. Diese Aussagen über die Sicherheit werden anhand der neuesten bekannten Verfahren sowie anhand der Rechenleistung heutiger Computer bestimmt und können sich bei unvorhersehbaren Entwicklungen natürlich auch stark verkürzen. Ab 2010 sieht die RegTP Verfahren vor, die längere Hashwerte erzeugen, wie z.B. das SHA-224, SHA-256, SHA-384 und das SHA-512 Verfahren, wobei die Zahlen im Namen für die Länge der Hashwerte in Bit stehen.

Genau wie für die Hashfunktionen schlägt die RegTP auch geeignete Signaturverfahren und Systemparameter für diese Verfahren vor. Laut RegTP geeignete Verfahren sind

3 das **RSA-Verfahren**, das nach seinen Erfindern Rivest, Shamir und Adleman benannt ist. Es beruht auf dem Faktorisierungsproblem für ganze Zahlen. Das heißt, dass es sehr schwierig ist, eine große Zahl in ihre Faktoren zu zerlegen. Die Erzeugung der Zahl ist dagegen sehr einfach, da sie durch einfache Multiplikation erzeugt werden kann.

4 das **DSA-Verfahren**, welches von der US-Regierung im Digital Signature Standard (DSS) herausgegeben wurde. Es beruht auf einem diskreten Logarithmus -Problem und ist eine Variante des ElGamal-Verfahrens. Weiterhin werden noch DSA-Varianten, die auf elliptischen Kurven basieren, vorgeschlagen.

Das bekannteste und im Moment wahrscheinlich auch meist verwendete Verfahren dürfte das RSA-Verfahren sein, welches auch schon in dieser Ausarbeitung vorgestellt wurde. Die RegTP gibt folgende Werte für die Systemparameter des RSA-Verfahrens vor, die voraussichtlich bis Ende 2010 sicher sein sollen.

Zeitraum Parameter	bis Ende 2007	bis Ende 2008	bis Ende 2009	bis Ende 2010
n	1024 (Mindestwert) 2048 (Empfehlung)	1280 (Mindestwert) 2048 (Empfehlung)	1536 (Mindestwert) 2048 (Empfehlung)	1728 (Mindestwert) 2048 (Empfehlung)

Abbildung 8.1: Systemparametervorgaben der RegTP für das RSA-Verfahren

Die Empfehlung ist aber schon heute, den Parameter n mit einer Länge von 2048 Bit zu verwenden, um sicher sein zu können, dass die Signatur nicht verändert oder manipuliert werden kann.
All diese Verfahren sind nicht absolut sicher, es ist grundsätzlich möglich die Signaturverfahren mittels geeigneter mathematischer Verfahren zu „knacken“. Die Sicherheit beruht darauf, dass es nicht in einer Zeit zu schaffen ist, die sich für den Kriminellen lohnt.

9 Identifizierungsmerkmale digitaler Signaturen

Digitale Signaturen werden in zertifikatsbasierte Signaturen und zertifikatsfreie Signaturen unterschieden.

9.1 Zertifikatsbasierte Signaturen

Die Identität des Verfassers ist in einem Zertifikat bestätigt, welches durch eine Zertifizierungsstelle ausgestellt wurde. Die Hauptbestandteile einer zertifkatsbasierten Signatur sind ein Hashwert und das Zertifikat.
In diesem Zertifikat ist die Identität der Person bestätigt.

9.2 Zertifikatsfreie Signaturen

Als zertifikatsfreie Signatur ist ein Bild der abgescannten handschriftlichen Unterschrift vorstellbar, welches in das Dokument eingefügt wird und so beim Berechnen des Hashwertes miteinbezogen wird.

10 Zertifikate

Um sicherzustellen, ob eine digitale Signatur auch wirklich von demjenigen stammt, der das Dokument unterzeichnet hat, wird der Hashwert des Dokuments mit einem privaten Schlüssel (Private-Key) verschlüsselt. Dieser verschlüsselte Hashwert ist nun die digitale Signatur, sie kann nur mit dem öffentlichen Schlüssel (Public-Key) des Unterzeichners wieder entschlüsselt werden.
Der private und der öffentliche Schlüssel sind über ein Zertifikat genau einer Person zugeordnet. Dies geschieht, indem man bei einer Zertifizierungsstelle (ZS) einen Antrag auf ein Zertifikat stellt und sich registrieren lässt. Anschließend muss man sich persönlich Ausweisen, z.B. mit dem Personalausweis. Nachdem man eindeutig identifiziert wurde wird ein Schlüsselpaar generiert und das Zertifikat ausgestellt. Dieses wird dann auf ein Trägermedium, z.B. eine spezielle Chipkarte, kopiert. Mit dieser Chipkarte kann man nun eine E-Mail, eine Dateien oder einen Server digital signieren.
Der Empfänger des signierten Dokuments erhält den öffentlichen Schlüssel entweder vom Unterzeichner selbst oder kann ihn aus einem öffentlichen Verzeichnis herunterladen.
X.509v3 ist der meistverwendete Standard für digitale Zertifikate. Dieser setzt voraus, dass es eine feste Hierarchie von Zertifizierungsstellen gibt.
Im Zertifikat sind folgende Informationen enthalten:

Zertifikat

- Version
- Seriennummer
- Algorithmen ID
- Aussteller
- Gültigkeit
    - Von
    - Bis
- Subject
- Subject Public Key Info
    - Public Key Algorithmus
    - Subject Public Key
- Eindeutige ID des Ausstellers (optional)

- Eindeutige ID des Inhabers (optional)
- Erweiterungen
- Zertifikat Signaturalgorithmus
- Zertifikat Signatur

In Abbildung 2 sieht man z.B. ein digitales Zertifikat, welches im Mozilla Firefox Browser enthalten ist. Bei diesem Browser sind schon bei der Installation eine Reihe von z.B. SSL-Serverzertifikaten installiert, von denen der Hersteller glaubt, sie seien vertrauenswürdig.

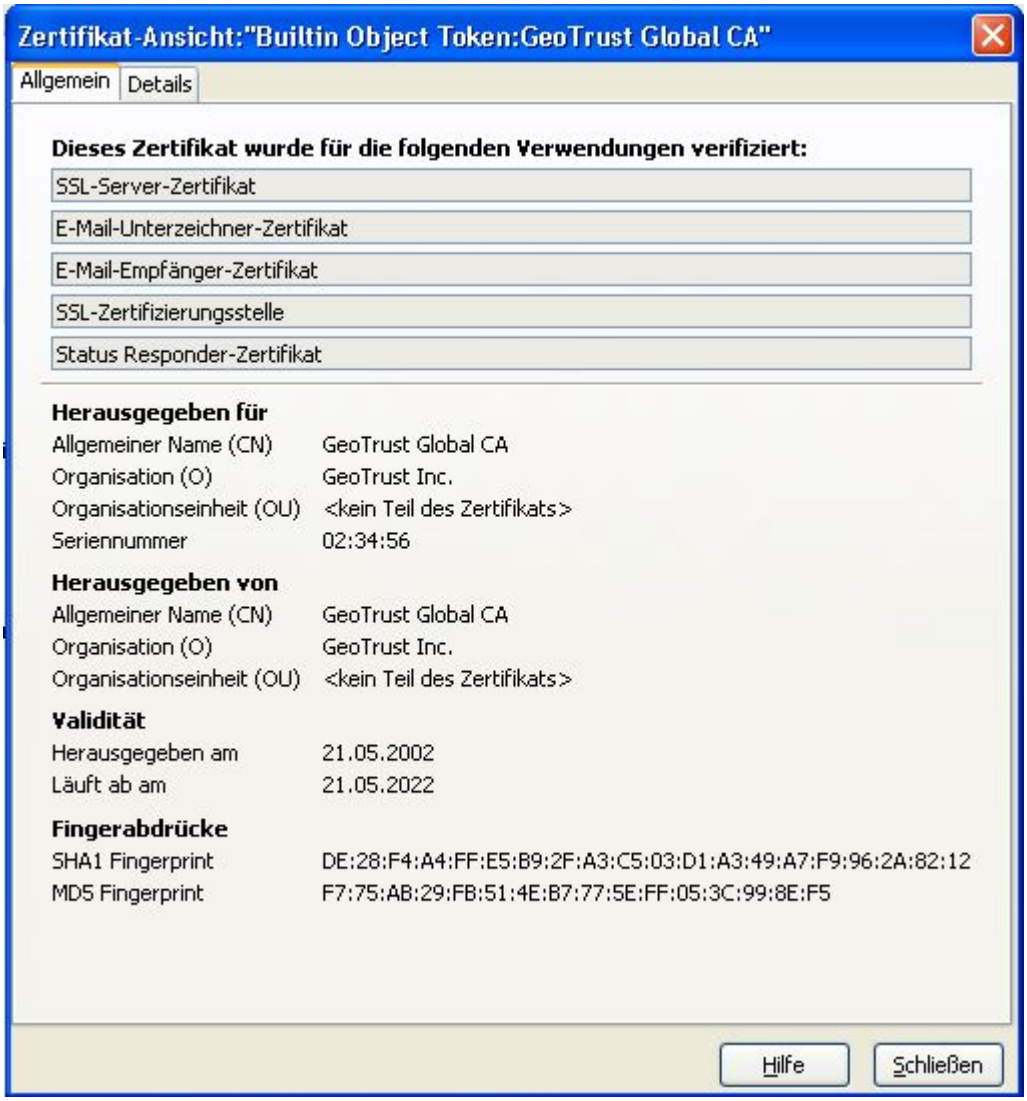

Abbildung 10.1: Vorinstalliertes Zertifikat aus dem Mozilla Firefox Browser

Wichtig für den Empfänger des Dokuments sind die Identität des Unterzeichners, die Gültigkeit des Zertifikats und der öffentliche Schlüssel des Unterzeichners. Außerdem muss das Zertifikat von einer vertrauenswürdigen Instanz ausgestellt worden

sein. Die ausstellende Instanz ist ebenfalls im Zertifikat namentlich erwähnt. Zusätzlich gibt es auch für diese vertrauenswürdige Instanz bzw. das Zertifikat eine digitale Signatur einer nächst höheren Instanz, denn in den meisten Fällen weiß man nicht, ob man der ausstellenden Instanz auch vertrauen kann. Es muss solange bei der nächst höheren Instanz die Vertrauenswürdigkeit hinterfragt werden, bis eine Instanz erreicht ist, der vertraut werden kann oder das obere Ende der Kette erreicht ist, das so genannte Wurzelzertifikat. In Deutschland ist die RegTP die höchste Instanz, also die Wurzelinstanz. Im Signaturgesetz (SiG) ist festgelegt, dass es in Deutschland nur eine zweistufige Hierarchie geben darf. Die Wurzelinstanz, die RegTP, zertifiziert ihrerseits die so genannten Zertifizierungsstellen (ZS), welche dann die Endanwender zertifizieren.

Die vertrauenswürdigen Zertifizierungsstellen werden von der RegTP veröffentlicht und können unter http://www.regtp.de/tech_reg_tele/start/in_06-02-04-00-00_m/index.html eingesehen werden. Das Wurzelzertifikat wird von der Behörde selbst ausgestellt und im Bundesanzeiger veröffentlicht. In Abbildung 3 ist eine solche Hierarchie von Zertifizierungsinstanzen zu sehen.

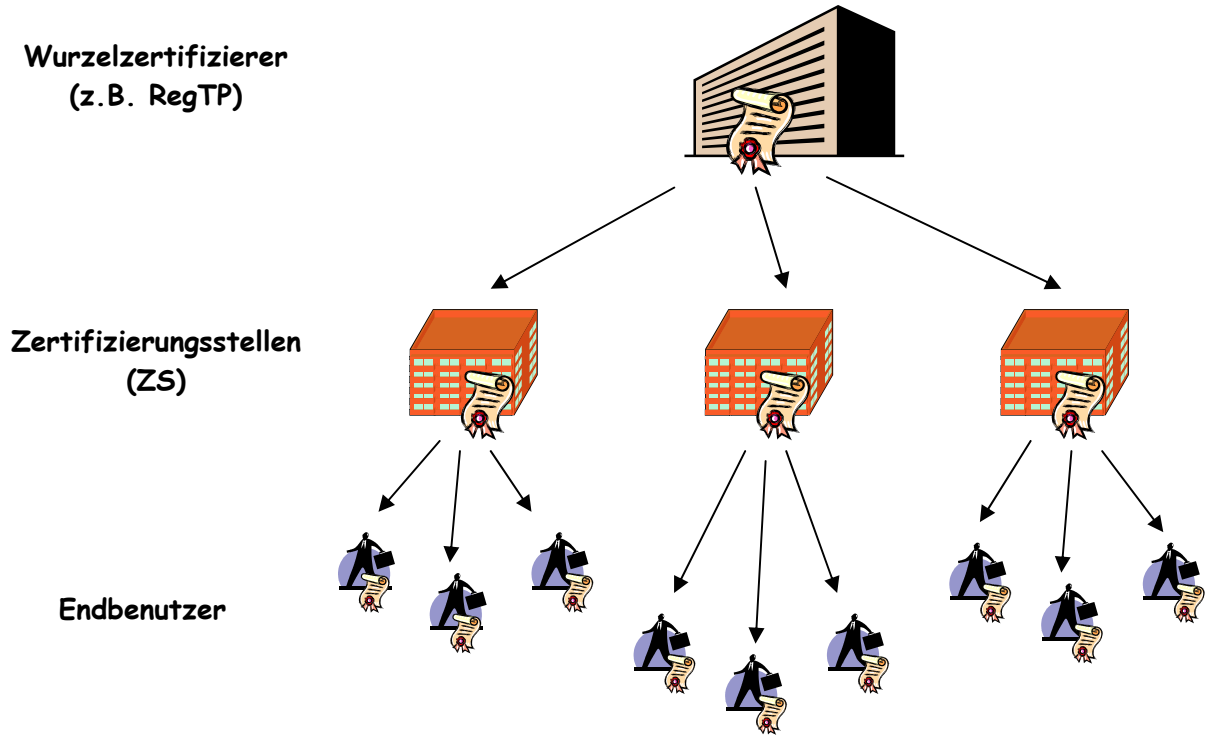

Abbildung 10.2: Zertifizierungshierarchie

Der Endbenutzer bekommt also sein Zertifikat von der Zertifizierungsstelle seiner Wahl. Zu diesem Zertifikat gehören ein privater und ein öffentlicher Schlüssel. Der

private Schlüssel wird dem Endbenutzer auf einer speziellen Chipkarte überreicht. Er kann seine Dokumente mit dieser Karte und einem 6-stelligen Pin, der die Karte vor fremden Zugriffen schützt, digital signieren. Der öffentliche Schlüssel wird an einer frei zugänglichen Stelle, z.B. einem Server der Zertifizierungsstelle, zum Herunterladen bereitgestellt. Die Zertifizierungsstelle stellt durch ihre digitale Signatur auf dem Zertifikat des Endbenutzers dessen Rechtmäßigkeit sicher. Die Zertifizierungsstelle ihrerseits stellt ihre Rechtmäßigkeit durch ein Zertifikat der Wurzelinstanz sicher, deren digitale Signatur sich auf diesem Zertifikat befindet.

Eine Zertifizierungsstelle hat folgende Aufgaben:

- **Schlüsselgenerierung** für die ZS und falls noch nicht vorhanden für die Teilnehmer
- **Schlüsselzertifizierung:** Zusammenstellen eines Zertifikats aus dem öffentlichen Schlüssel, den Teilnehmerdaten und weiteren Daten
- **Personalisierung:** Zusammenfassen des Schlüsselpaares und des Zertifikates auf der Chipkarte
- **Identifizierung und Registrierung:** Mittels des Personalausweises werden die Teilnehmer identifiziert und registriert
- **Verzeichnisdienst:** Das Zertifikat wird in einem öffentlichen Verzeichnis zur Verfügung gestellt

Neben der Aufgabe, die Zertifikate der Teilnehmer öffentlich zur Verfügung zu stellen, hat der Verzeichnisdienst noch die Aufgabe, so genannte Sperrlisten (CRL, certificate revocation list) zu führen. In diesen Listen werden Zertifikate geführt, die ihre Gültigkeit verloren haben. Dies kann durch Ablauf des Ausstellungszeitraums oder z.B. durch den Verlust des privaten Schlüssels geschehen. Die Verwaltung der CRL ist sehr aufwendig, da sie immer auf dem aktuellen Stand gehalten werden muss.
Eine Aufgabe, die bisher noch nicht erwähnt wurde, ist die Erstellung von **Zeitstempeln**. Ein Zeitstempel ist ein Nachweis, dass ein bestimmtes Dokument zu einer bestimmten Zeit eingegangen ist. Ein Beispiel ist die Datumsangabe im Briefkopf eines Briefes, die angibt wann der Brief erstellt wurde. Wobei bei dieser Methode der Verfasser des Briefes auch ein falsches Datum einfügen könnte. Beim elektronischen Zeitstempel, der durch eine vertrauenswürdige Instanz ausgestellt wird, kann der Empfänger sicher sein, dass das Dokument auch zu dem genannten Zeitpunkt be-

endet und seitdem unverändert geblieben ist. Auch hier wird häufig nur der Hashwert des Dokumentes mit einer Zeitangabe und einer digitalen Signatur versehen.

11 Zertifikatsklassen

Von manchen Zertifizierungsstellen (z.B. der TrustCenter AG) werden die angebotenen Zertifikate noch in unterschiedliche Klassen eingeteilt. Jede Klasse hat eine andere Sicherheitsstufe bzw. eine bessere Sicherstellung der Identität des Zertifizierten.

Die Klassen sind:

- **Class 0**: Demo-Zertifikat mit einer Gültigkeit von 30 Tagen für Testzwecke.
- **Class 1**: Zertifikat mit geringer Sicherheit, da nur die Existenz einer E-Mail.Adresse geprüft wird und ob der Benutzer Zugriff auf dieses E-Mail-Postfach hat. Da keine persönliche Prüfung stattfindet, kann ein Class 1-Zertifikat sofort über das Internet ausgestellt werden.
- **Class 2**: Ein Zertifikat mit mittlerer Sicherheit, welches für Privatpersonen und Unternehmen gedacht ist. Es beinhaltet ebenfalls keine persönliche Identitätsfeststellung. Es reicht, wenn das Unternehmen eine Kopie des Handelsregisterauszuges oder die Privatperson eine Kopie des Personalausweises und einen schriftlichen Auftrag einreicht. Es besteht dann eine gewisse Sicherheit, dass die Person bzw. das Unternehmen wirklich existieren.
- **Class 3**: Bei einem Class 3-Zertifikat handelt es sich um ein Zertifikat mit hoher Sicherheit. Neben der E-Mail-Überprüfung muss sich die Person persönlich bei der Zertifizierungsstelle mit dem Personalausweis oder dem Reisepass identifizieren. Die Angaben im Personalausweis werden geprüft, damit der Zertifizierer sicher sein kann, dass die Person existiert und die Angaben im Zertifikat richtig sind. Für Unternehmen ist es erforderlich, dass unter anderem ein beglaubigter Auszug aus dem Handelsregister eingereicht wird, da bei diesem Zertifikat die juristische Person überprüft werden muss.
- **Class 4**: Das Zertifikat mit der höchsten Sicherheit. Bei diesem Zertifikat unterliegen der Zertifikatsherausgeber sowie der ganze Prozess der Zertifizierung einer staatlichen Kontrolle. Diese Klasse wird aber aufgrund der geringen Nachfrage nicht immer angeboten.

12 Gültigkeitsdauer von Zertifikaten

Zertifikate sind üblicherweise zwei bis drei Jahre gültig. Es gibt aber auch Zertifikate, die fünf Jahre gültig sind. Nach Ablauf der Gültigkeitsdauer muss die Zertifizierungsstelle die Zertifikate zum Zweck der Identifizierung noch weitere fünf Jahre aufbewahren.
Die Gültigkeit der Zertifikate ist zeitlich begrenzt, da man davon ausgeht, dass die verwendeten Signaturalgorithmen nach einigen Jahren überholt sind und „geknackt“ werden können. Wenn dies geschieht, kann nicht mehr für die Unverfälschtheit des Dokuments garantiert werden. Wie oben beschrieben, geht man davon aus, dass die Algorithmen sechs Jahre sicher sind. Aus Sicherheitsgründen wird die maximale Gültigkeit aber auf fünf Jahre beschränkt. Es müssen also Vorkehrungen getroffen werden, dass nach Ablauf der Zertifikate die Gültigkeit der digitalen Signaturen noch gewährleistet werden kann.
Damit ein Dokument seine Gültigkeit nicht nach Ablauf des Zertifikats verliert, besteht die Möglichkeit, dass der Unterzeichner das Dokument nachsigniert, um die Integrität und die Identität des Dokuments bzw. des Unterzeichners zu verlängern, wobei er ein neues Zertifikat benutzt.
Eine weitere Möglichkeit ist, dass Dokument inklusive seiner digitalen Signatur an ein elektronischen Archiv zu übergeben. In diesem elektronischen Archiv erhalten das signierte Dokument sowie die digitale Signatur einen Zeitstempel. Ab diesem Zeitpunkt ist das Archiv dafür verantwortlich, dass der Inhalt des Dokuments bzw. der digitalen Signatur nicht verfälscht werden kann. Der Begriff für ein solches elektronisches Archiv lautet „revisionssicheres Archiv“.

13 S/MIME und OpenPGP

Für die Verschlüsselung und Signierung von E-Mail gibt es zwei wichtige Standards, die auf unterschiedlichen Zertifikatsmodellen aufbauen.
Der Secure Multipurpose Internet Mail Extension-Standard (S/MIME) basiert auf dem im oberen Abschnitt beschriebenen hierarchischen Public-Key-Verfahren, indem das Zertifikat von einer Zertifizierungsstelle ausgegeben wird. Es handelt sich dabei um ein X.509 Zertifikat, wie es im vorigen Abschnitt schon beschrieben wurde. Der S/MIME-Standard wird von den meisten E-Mail-Programmen von Haus aus unterstützt.

Der OpenPGP-Standard (Pretty Good Privacy) ist der wohl meistverbreitete Standard auf der Welt. Bei ihm werden so genannte PGP-Zertifikate ausgegeben, die sich dadurch unterscheiden, dass sie von mehreren Personen oder Institutionen zertifiziert werden können, wogegen bei dem X.509 nur eine Institution zertifizieren kann. Außerdem ist die Angabe einer E-Mail Adresse im X.509 Standard nur optional, was zu Schwierigkeiten bei der Zuordnung zu einem Client führen kann.
Beim OpenPGP-Standard gibt es kein hierarchisches Public-Key-Verfahren. Es basiert auf dem so genannten *Web of Trust;* das heißt, dass die User sich gegenseitig zertifizieren bzw. das Vertrauen aussprechen. Kennen sich zum Beispiel Alice und Bob und tauschen auch signierte E-Mails aus, vertrauen sie sich gegenseitig. Bekommt nun Alice eine signierte Nachricht von Charlie, weiß sie nicht, ob sie ihm vertrauen kann. Da aber Bob und Charlie einander vertrauen und Alice Bob vertraut, kann Alice auch Charlie vertrauen.
Beim PGP Standard werden die Zertifikate auf HTML-Key-Servern hinterlegt. Es gibt auf der ganzen Welt solche HTML-Key-Servern, die sich gegenseitig updaten und dafür sorgen, dass auf allen Servern sämtliche Zertifikate vorhanden sind. Man kann seine Zertifikate aber auch auf mehreren HTML-Key-Servern hinterlegen, wenn man sicher gehen will, dass es wirklich auf allen Servern vorhanden ist, da der Austausch zwischen den Servern nicht immer richtig funktioniert. Dagegen wird bei S/MIME nur ein Server von der Zertifizierungsstelle betrieben, auf dem die Zertifikate öffentlich zur Verfügung gestellt werden.

14 Gefahren und Probleme der elektronischen Signaturen

Die größte Gefahr bei der Verwendung von elektronischen Signaturen besteht darin, dass ein Unberechtigter in den Besitz des privaten Schlüssels gelangen kann. Dies passiert vor allem durch Unachtsamkeiten des Schlüsselinhabers. Wenn dieser zum Beispiel den privaten Schlüssel auf der Festplatte seines Computers abspeichert, besteht eine ernstzunehmende Gefahr, dass dieser durch entsprechende Software ausspioniert werden kann. Aber auch nichttechnische Gefahren sind hier zu erwähnen. Ist der Schlüssel auf einer Chipkarte gespeichert, so muss diese natürlich an einem sicheren, für Diebe unzugänglichen Ort aufbewahrt werden.
Der Diebstahl des privaten Schlüssels ist deshalb so gefährlich, da der Dieb sich als der Schlüsselbesitzer ausgeben kann. Es gibt keine Möglichkeit zu unterscheiden, ob der Dieb oder der eigentliche Besitzer des Schlüssels eine Signatur angebracht hat. Dies ist auch der wesentliche Unterschied zu einer herkömmlichen handschriftlichen

Unterschrift. Eine gefälschte Unterschrift, ist die Fälschung auch noch so gut, unterscheidet sich immer vom Original. Eine missbräuchlich angebrachte Signatur ist jedoch exakt identisch mit dem Original. Es ist zu vergleichen mit einem gestohlenen Siegel.

Insbesondere Besitzer von Zertifikaten, die qualifizierte Signaturen erzeugen, müssen sich der besonderen Bedeutung des Schutzes des privaten Schlüssels bewusst sein. Denn vor Gericht gilt, dass der Besitzer beweisen muss, dass sein Schlüssel von einem Fremden angewendet wurde. Dies ist jedoch in der Praxis eher schwierig. Aber gerade dieser Punkt ist besonders wichtig, um elektronische Signaturen weit zu verbreiten. Denn nur wenn man sich darauf verlassen kann - notfalls auch vor Gericht -, dass der Unterzeichner auch derjenige ist, auf den das Zertifikat ausgestellt wurde, werden sich elektronische Signaturen im Alltag durchsetzen.

Bei fortgeschrittenen Signaturen ist dieser Sachverhalt jedoch genau umgekehrt. Die Gegenseite muss beweisen, dass der Besitzer selbst die Signatur angebracht hat. Für reine Onlinegeschäfte, bei denen sich beide Vertragsparteien nicht persönlich sehen, ist diese Art der Signatur nicht geeignet. Praktikabel ist dies zum Beispiel bei Paketdiensten, hier kann der Zusteller bestätigen, dass der Betreffende selbst die Signatur angebracht hat und kein Dritter.

Aber generell sollte dem Benutzer bei allen Signaturen klar sein, dass die Signatur nur begrenzt gültig ist. Dies hängt davon ab, wie lange das zugehörige Zertifikat gültig ist. Zertifikate sind nur begrenzt gültig, weil es theoretisch möglich wäre, den privaten Schlüssel durch stupides Ausprobieren sämtlicher möglicher Schlüssel zu erhalten. Die dafür notwendige Zeit legt die Gültigkeit eines Zertifikats fest.

Ein weiterer Unterschied von elektronischen Signaturen zu herkömmlichen handschriftlichen Unterschriften besteht darin, dass man nicht direkt sieht, was man signiert. Der Benutzer muss sich darauf verlassen, dass das zum Signieren verwendete Programm auch wirklich den Text anzeigt, der signiert wird. Denkbar wäre hierbei, dass durch einen Dritten das Programm so manipuliert wird, dass ein völlig anderer Text signiert wird, als der angezeigte.

14.1 Standard-Zertifikate in Internetbrowsern

In jedem Internetbrowser werden Stamm-Zertifikate von verschiedenen Zertifizierungsstellen standardmäßig als vertrauenswürdig eingestuft. Vertrauenswürdig heißt, dass diese Zertifikate automatisch akzeptiert werden. Alle Zertifikate von nicht als vertrauenswürdig eingestuften Stamm-Zertifikaten erzeugen eine Warnmeldung, in der abgefragt wird, ob das Zertifikat akzeptiert werden soll.

Der Betreiber einer Internetseite ist bestrebt, dass beim Aufruf seines Internetangebots keine Warnmeldung erscheint. Aus diesem Grund wird er sich ein Zertifikat ausstellen lassen. Er wird dies allerdings nur bei einer Zertifizierungsstelle tun, die auch standardmäßig von den gängigen Internetbrowsern als vertrauenswürdig eingestuft wird. So erscheint keine Warnmeldung mehr beim Endbenutzer. Für ein solches Zertifikat muss man natürlich Geld bezahlen.

Die Zertifizierungsstellen wiederum sind daran interessiert, dass sie in die Liste der Standardzertifikate aufgenommen werden, denn so lassen sich deren Zertifikate besser und auch teurer verkaufen.

Der Browserhersteller lässt sich die Aufnahme in die Liste der vertrauenswürdigen Zertifikate auch bezahlen. Dies ist auch der Grund, warum Warnmeldungen von nicht vertrauenswürdig eingestuften Zertifikaten besonders abschreckend formuliert werden. Nur so ist gewährleistet, dass der Benutzer abgeschreckt wird und deshalb der Internetseitenanbieter ein Zertifikat kauft.

Bei dieser Kommerzialisierung leidet jedoch die eigentliche Aufgabe dieses Systems - die Sicherheit. Schafft es eine Zertifizierungsstelle durch Zahlung eines großen Betrags in die Liste aufgenommen zu werden, die die Identitäten ihrer Zertifikatsinhaber nur mangelhaft prüft, so ist die gesamte Zertifikatsprüfung sinnlos. Denn ein fragwürdiges Stamm-Zertifikat reicht aus, um das System auszuhebeln. Jedes Zertifikat der vertrauenswürdigen Stamm-Zertifikate wird automatisch akzeptiert, also auch das der fragwürdigen Zertifizierungsstelle. Deshalb muss jeder Benutzer die Liste der vertrauenswürdigen Stamm-Zertifikate manuell überprüfen. Dies ist in der Praxis jedoch nur mit großem Aufwand bzw. gar nicht möglich, da der unversierte Benutzer nicht einschätzen kann, welche Stamm-Zertifikate seriös sind.

15 Literaturverzeichnis

[1] RICHTER, HELMUT: *Verschlüsselung, digitale Signaturen, Zertifikate*. Leibniz Rechenzentrum der Bayerischen Akademie der Wissenschaften. Juni 2004.

[2] PROJEKTGRUPPE E-GOVERNMENT IM BSI: *Verschlüsselung und Signatur*. Bundesamt für Sicherheit in der Informationstechnik. April 2005. http://www.bsi.bund.de/fachthem/egov/6.htm

[3] REGTP, REFERAT 15 IS: *Die digitale Signatur.* Regulierungsbehörde für Telekommunikation und Post. http://www.protext.de/allgemein/Erkl%C3%A4rung%20DigSig.pdf

[4] REISEN, ANDRE: *Digitale Signaturen*. Bundesamt für Sicherheit in der Informationstechnik. Juni 1998.

[5] REGTP: *Übersicht über geeignete Algorithmen.* Bundesanzeiger, 30. März 2005 S. 4695-4696. http://www.regtp.de/tech_reg_tele/in_06-02-02-00-00_m/03/index.html

[6] WIKIPEDIA, Deutschland. http://de.wikipedia.org

[7] NETZWERK ELEKTRONISCHER GESCHÄFTSVERKEHR: *Präsentation: Elektronische Signaturen.* http://www.ec-sicherheit.de/downloads/files/Vortraege/Elektronische%20Signatur.ppt

[8] SCHMOLDT, ROLF: *Leitfaden Elektronische Signatur.* Frankfurt am Main, Juni 2005 http://www.signature-perfect.com/docs/Leitfaden_Elektronische_Signatur.pdf