Die Rolle von Verschlüsselung, digitalen Signaturen und digitalen Zertifikaten beim E-Commerce

Arno Hornberger
a_hornbe@informatik.uni-kl.de

Seminararbeit im Sommersemester 2001

Arbeitsgruppe
Datenbanken und Informationssysteme

Universität Kaiserslautern

Inhalt

0. Motivation

Hat sich die Nutzung und Verbreitung des Internet zunächst nur in wissenschaftlichen und militärischen Einrichtungen abgespielt, so wurde das Internet mit zunehmender Öffnung für die private Nutzung auch stetig interessanter für kommerzielle Interessen. Redete man hier zunächst von Geschäften mit relativ kleinem Volumen (z. B. dem Verkauf/Kauf von Büchern, CDs), so ist es heute bereits möglich, Autos über das Internet zu kaufen oder finanzielle Transaktionen in nahezu beliebigem Umfang über das Internet zu tätigen.

Mit der Wandlung der Nutzung des Internet von wissenschaftlichen und nichtkommerziellen Zwecken hin zu privaten und geschäftlichen Belangen geht auch ein gestiegenes Sicherheitsbedürfnis für private und kommerzielle Nutzer einher. Dies betrifft neben dem Verlangen nach Schutz der Privatsphäre für den einzelnen Nutzer auch das Verlangen, Geschäfte über das Internet mit ähnlichen Mechanismen wie in der realen Welt und unter Garantie ähnlicher (oder gar besserer) Sicherheit abwickeln zu können. Verträge bürgen bei den traditionellen Formen der Geschäftsabwicklung für Rechtsverbindlichkeit und Sicherheit. Eine zentrale Frage ist daher, ob und wie es möglich ist, ein elektronisches Äquivalent zu einem Vertrag in Papierform zu erstellen.

Ein Kernelement bei der Beantwortung all dieser Fragen sind kryptographische Verfahren und deren spezielle Anwendung für digitale Signaturen.

1. Kryptographische Verfahren

1.1. Vorbemerkung

Unter Kryptographie versteht man die Wissenschaft von der Verschlüsselung von Daten unter der Zuhilfenahme von mathematischen Verfahren. Kryptographie erlaubt dabei die Speicherung oder Übertragung von Nachrichten in einer Art und Weise, daß niemand als der beabsichtigte Empfänger diese Nachricht entschlüsseln kann. Sicherheit soll durch kryptographische Verfahren also in erster Linie durch Geheimhaltung vor unbefugten Personen erreicht werden.

Der Einsatz kryptographischer Verfahren reicht zurück bis in die Antike, wo bereits Julius Cäsar wichtige Botschaften mithilfe eines simplen Algorithmus verschlüsselte, der je einen Buchstaben in der Botschaft durch einen Folgebuchstaben ersetzte. Verschlüsselungsverfahren wurden und werden in großem Maße für militärische Zwecke und Geheimdienste eingesetzt, so daß viele Fortschritte in der kryptographischen Forschung auf diese Einrichtungen zurückgehen.

Im vergangenen Jahrhundert waren Weiterentwicklungen in der Kryptographie vor allem durch Fortschritte in der Mathematik verbunden mit der Entwicklung der Computertechnik möglich. Computer ermöglichten dabei erstmals, auch komplizierte, bessere Verschlüsselungsverfahren in einer akzeptablen Geschwindigkeit zu verwenden.

Es ist nicht leicht, die Güte eines kryptographischen Verfahrens zu beurteilen. Oft kann es Jahre dauern, bis sich durch die Kryptanalyse (die Wissenschaft von der Erforschung der Sicherheit kryptographischer Verfahren) ein vermeintlich sicheres Verschlüsselungsverfahren als leicht zu brechen herausstellt. Daher kann die Güte eines kryptographischen Verfahrens im allgemeinen nicht als endgültige Größe betrachtet werden, sondern sie sollte immer in Relation zum Stand der wissenschaftlichen Erkenntnisse sowie der technischen Möglichkeiten zum Betrachtungszeitpunkt gesetzt werden. Um dennoch eine Orientierung zu bieten, kann man kryptographische Verfahren

grob in starke und schwache Verfahren einteilen. Die Stärke eines Verfahrens wird dabei durch die Zeit gemessen, die ein potentieller Angreifer ohne entsprechenden Schlüssel zum Entschlüsseln einer gegebenen Nachricht brauchen würde. Im Extremfall geschieht dies durch Durchprobieren aller möglichen Schlüssel (Brute-Force). Starke Verfahren zeichnen sich durch einen hohen bis sehr hohen Zeitaufwand für einen kryptographischen Angreifer aus (nicht selten einige tausend Jahre), schwache Verfahren durch einen entsprechend niedrigen Aufwand. Die Stärke des verwendeten Verfahrens ist dabei in der Regel auch in hohem Maße abhängig von der Länge und Güte (Werteverteilung) der verwendeten Schlüssel.

Kryptographische Verfahren ermöglichen zwar weitgehende Sicherheit im Sinne der Geheimhaltung, können aber im Sinne der Anforderungen an Systeme zur kryptographisch gesicherten elektronischen Kommunikation nach Lynch/Lundquist [4] nur als Teilkomponente eines umfassenderen Systems gesehen werden. Elemente eines solchen Systems sind u. a. kryptographische Verfahren, Vorschriften für deren Anwendung, rechtliche Vorschriften und Einrichtungen zur Zertifikation (vgl. Abschnitt 4 und 5).

Lynch/Lundquist nennen folgende Anforderungen an Systeme zur kryptographisch gesicherten elektronischen Kommunikation:

- **Identification (Identifikation)**
  Möglichkeit der sicheren Identifizierung des Absenders einer Botschaft (vgl. Abschnitt 3)
- **Authentication (Echtheit)**
  Prüfung auf elektronische Unversehrtheit der verschickten Nachricht zum Schutz vor Manipulation (vgl. Abschnitt 2)
- **Verification (Beglaubigung)**
  Hierunter vesteht man die Möglichkeit, Identifikation und Echtheit einer Botschaft zu gewährleisten. Sind beide Anforderungen erfüllt, so kann man der Botschaft völlig vertrauen.
- **Nonrepudiation (Unleugbarkeit)**
  Die Fähigkeit eines Systems, sicherzustellen, daß der Versand oder Empfang einer Botschaft nicht abgestritten werden kann.
- **Privacy (Geheimhaltung)**
  Das System kann die Botschaft effektiv vor Unbefugten verstecken.

Systeme, die alle diese Anforderungen hinreichend erfüllen gelten nach Lynch/Lundquist als sicher.

Kryptographische Verfahren lassen sich nach der Art der Schlüsselverteilung in symmetrische und asymmetrische Verfahren einteilen. Hybride Verfahren stellen eine Kombination aus symmetrischen und asymmetrischen Verfahren dar.

1.2. Symmetrische Verfahren (Private-Key-Verfahren)

Symmetrische Verfahren zeichnen sich durch ein einfaches Verfahrensschema aus und wurden infolgedessen historisch gesehen auch zuerst entwickelt.

Die Funktionsweise symmetrischer Verfahren soll hier anhand eines einfachen Beispiels verdeutlicht werden.

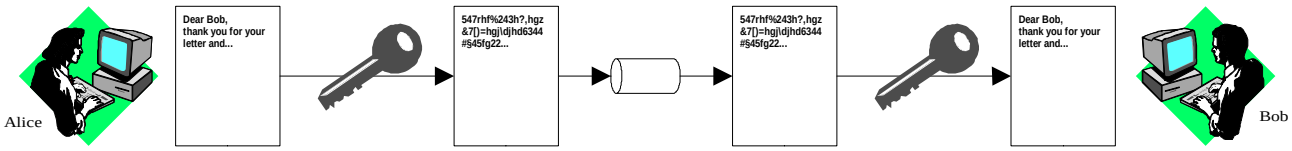

Abb. 1: Kommunikation mit symmetrischer Verschlüsselung

Alice will Bob eine geheime Nachricht schicken. Weil niemand anders als Bob diese Nachricht lesen soll, vereinbaren die beiden einen Code zur Verschlüsselung der Nachricht: Bevor Alice die Botschaft abschickt ersetzt sie jeden Buchstaben darin durch den Folgebuchstaben im Alphabet. Nun schickt sie die Nachricht an Bob. Der weiß, wie Alice die Nachricht verschlüsselt hat, und kann jetzt diese Verschlüsselung rückgängig machen und die Nachricht lesen. Eine dritte Person, die die Nachricht bei der Übertragung mithört, kann mit der verschlüsselten Nachricht wenig anfangen, da die nötige Kenntnis über die Art des verwendeten Verschlüsselungsverfahrens und den verwendeten Schlüssel fehlt.

Solche Verfahren bezeichnet man als symmetrisch, da zur Ver- und Entschlüsselung der gleiche Schlüssel verwendet wird. Bedeutende Vertreter symmetrischer Verschlüsselungsverfahren sind DES (1974), IDEA (1990), Blowfish (1994) und CAST [9].

Die beschriebene Art der verschlüsselten Kommunikation mit symmetrischen Verfahren bringt einige Probleme mit sich. So benötigen Alice und Bob zur kryptographisch gesicherten Kommunikation beide den gleichen Schlüssel. Wohnt Alice in der Nähe von Bob, so kann sie ihm den Schlüssel persönlich übergeben. In vielen Fällen ist dies allerdings nicht möglich, sodaß Alice Bob den Schlüssel irgendwie übermitteln muß. Dies kann z. B. über den Postweg, das Internet oder das Telefon geschehen. All diesen Möglichkeiten der Übermittlung des Schlüssels ist aber gemein, daß ein dritter mit genügend krimineller Energie den Schlüssel bei der Übertragung leicht abfangen und die spätere verschlüsselte Kommunikation mit diesem Schlüssel abhören kann (Man-in-the-middle-Attack).

Alice und Bob bräuchten für eine sinnvolle Anwendung der symmetrischen Verschlüsselung also einen sicheren Kanal zur Übermittlung des geheimen Schlüssels (z. B. ein abhörsicheres Telefon). Stünde ein solcher Kanal zur Schlüsselübermittlung aber zur Verfügung, so bräuchten Alice und Bob keine Verschlüsselung und das Verfahren würde sich selbst ad absurdum führen.

Steht ein sicherer Kanal zur Verfügung, so kann es aus Kostengründen dennoch sinnvoll sein, mittels Verschlüsselung über den unsicheren Kanal miteinander zu kommunizieren (vgl. Abschnitt 1.4.). Durch die Tatsache, daß Alice und Bob über den gleichen Schlüssel verfügen, ergeben sich für einen potentiellen Schlüsseldieb nun aber ungefähr doppelt so viele Möglichkeiten, sich des geheimen Schlüssels zu bemächtigen.

Trotz der beschriebenen Unzulänglichkeiten der symmetrischen Verfahren werden diese (wenn auch in Kombination mit anderen Verfahren, vgl. Abschnitt 1.4.) noch heute eingesetzt. Dies liegt im wesentlichen an der hohen Geschwindigkeit der symmetrischen Verfahren, die selbst die verschlüsselte Übertragung von multimedialen Inhalten in Echtzeit über das Internet ermöglichen. Ein weiterer Vorteil symmetrischer Verfahren liegt in einem ganz bestimmten Einsatzzweck begründet, nämlich dem der verschlüsselten Archivierung von Daten. Hier findet im allgemeinen keine Übertragung der Daten statt, sodaß sich die Problematik des Schlüsseltransfers hier nicht ergibt und symmetrische Verfahren ausreichend Schutz bieten können.

1.3. Asymmetrische Verfahren (Public-Key-Verfahren)

Die Probleme der symmetrischen Verfahren ergeben sich im wesentlichen aus der Notwendigkeit des Schlüsseltransfers, da der gleiche Schlüssel zum Ver- und Entschlüsseln benötigt wird. Diese Feststellung zeigt gleichzeitig aber auch eine Lösungsmöglichkeit für diese Problematik auf, wie sie von den asymmetrischen Verfahren verwandt wird, nämlich die Aufteilung des Schlüssels in einen frei zugänglichen öffentlichen und einen privaten Teil.

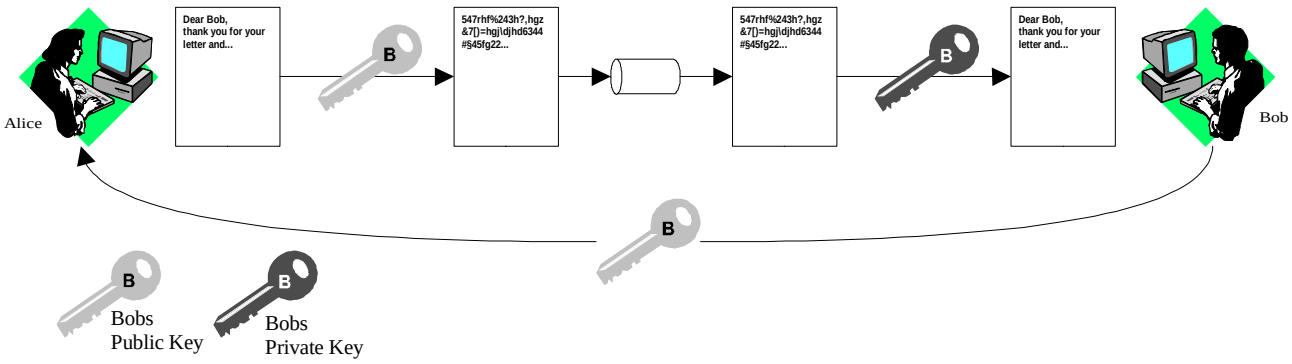

Abb. 2: Kommunikation mit asymmetrischer Verschlüsselung

Bei der Verwendung von asymmetrischen Verschlüsselungsverfahren besitzen Alice und Bob je ein Schlüsselpaar bestehend aus einem (frei zugänglichen) öffentlichen und einem privaten Schlüssel, der jeweils nur seinem Besitzer zugänglich ist. Ein Rückschluß von einem öffentlichem Schlüssel auf den zugehörigen privaten Schlüssel darf dabei nicht oder nur mit extrem hohem Aufwand möglich sein.

Will Alice oder irgendeine andere Person nun eine Nachricht an Bob schicken, so benutzt sie dessen öffentlichen Schlüssel aus einem öffentlichen Schlüsselverzeichnis, um die Nachricht zu verschlüsseln. Nur Bob kann die verschlüsselte Botschaft anschließend mit seinem privaten Schlüssel entschlüsseln.

Das Problem des Schlüsseltransfers, wie es bei den symmetrischen Verfahren vorherrscht, besteht hier nicht mehr, da der öffentliche Schlüssel immer nur in eine Richtung, in diesem Fall nämlich zur Verschlüsselung, benutzt werden kann. Die Asymmetrie liegt in der Verwendung von zwei Schlüsselarten begründet: Eine mit einer Art von Schlüssel (privat/öffentlich) verschlüsselte Botschaft kann dabei nur mit ihrem entsprechenden Gegenstück entschlüsselt werden.

Als bedeutendste Vertreter der asymmetrischen Verschlüsselungsverfahren kann man Diffie-Hellman (1976) und RSA (1978) nennen (vgl. [9]). Die Sicherheit von RSA basiert dabei auf dem schwierigen mathematischen Problem der Primfaktorzerlegung von großen Zahlen, die Sicherheit von Diffie-Hellman beruht auf der Schwierigkeit, diskrete Logarithmen über einem endlichen Körper zu berechnen.

Asymmetrische Verfahren bieten eine symmetrischen Verfahren ähnliche Stärke (jedoch bei sehr viel größerer Schlüssellänge) und lösen das Problem der Schlüsselübermittlung. Durch die notwendige große Schlüssellänge und den hohen Rechenaufwand bei der Verschlüsselung sind sie jedoch symmetrischen Verfahren hinsichtlich ihrer Laufzeit nicht selten um den Faktor tausend unterlegen. Darin liegt auch der Grund, daß asymmetrische Verfahren in der Regel nicht in der oben beschriebenen Form eingesetzt werden.

Mit der Einführung des Konzepts der öffentlichen Schlüssel ergibt sich bei deren zentraler Speicherung in einem frei zugänglichen Schlüsselverzeichnis desweiteren das Problem, wie eine verläßliche Zuordnung zwischen öffentlichem Schlüssel und dessen Eigentümer möglich ist (vgl. Abschnitt 3).

1.4. Hybride Verfahren

Hybride Verfahren vereinen den Vorteil der hohen Geschwindigkeit von symmetrischen Verfahren mit der Sicherheit der asymmetrischen Verfahren bei der Schlüsseldistribution. Dies wird durch einen kombinierten Einsatz eines symmetrischen und eines asymmetrischen Verfahrens erreicht.

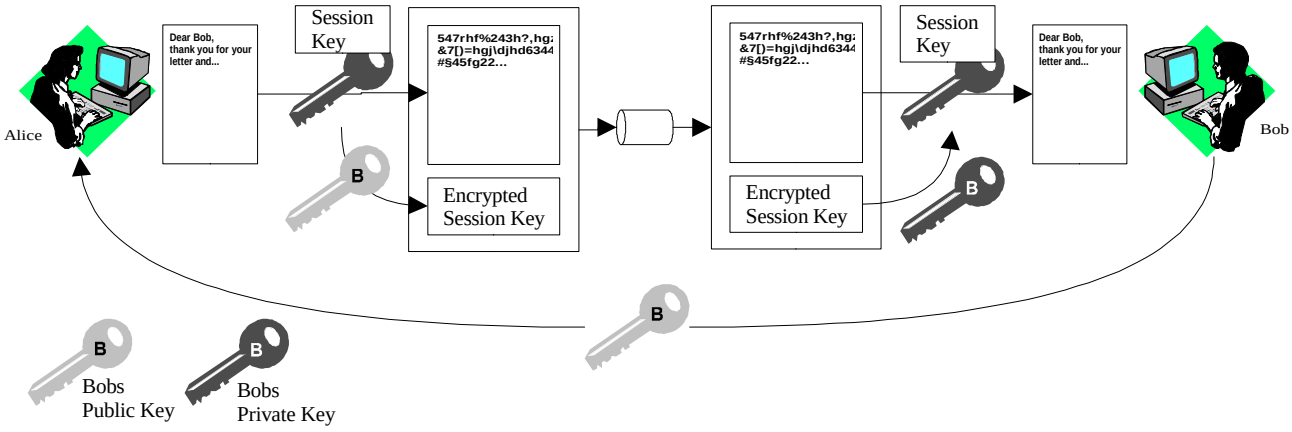

Abb. 3: Kommunikation mit hybrider Verschlüsselung

Will Alice eine Nachricht an Bob schicken, so erzeugt sie für diese Nachricht einen privaten Schlüssel (Session-Key) für das benutzte symmetrische Verfahren. Alice verschlüsselt die Nachricht an Bob mit dem symmetrischen Verfahren unter Verwendung des Session-Key und verschlüsselt anschließend den Session-Key mit dem öffentlichen Schlüssel von Bob. Nun schickt sie den verschlüsselten Session-Key zusammen mit der verschlüsselten Nachricht an Bob. Nur Bob kann mit seinem privaten Schlüssel den verschlüsselten Session-Key entschlüsseln und mit diesem die Botschaft lesen.

Die hohe Geschwindigkeit und Sicherheit der hybriden Verfahren ergibt sich daraus, daß nur der Session-Key, der in der Regel kurz im Vergleich zur zu übermittelnden Botschaft ist, mittels eines Public-Key-Verfahrens verschlüsselt wird. Jemand der die Botschaft lesen wollte, müßte entweder versuchen durch Brute-Force-Angriff an die verschlüsselte Botschaft zu gelangen (Bruch des symmetrischen Verfahrens), oder aber den Session-Key zu entschlüsseln, was gleichbedeutend mit dem Bruch des Public-Key-Verfahrens wäre. Durch Wahl geeigneter Verschlüsselungsverfahren und Schlüssellängen kann man beide Angriffsszenarien nahezu ausschließen.

Das weit verbreitete PGP (Pretty Good Privacy) von Phil Zimmermann setzt hybride Verfahren in der beschriebenen Form ein. Als symmetrische Verfahren kommen dabei zur Zeit IDEA, CAST und 3DES (Triple-DES) zum Einsatz, als Public-Key-Verfahren können RSA und DH (Diffie-Hellman) benutzt werden (vgl. [10]).

2. Digitale Signaturen

2.1. Bedeutung digitaler Signaturen und rechtliche Aspekte

Ohne rechtsverbindliche Vereinbarungen ist kein sicherer Handel möglich. Dies gilt sowohl in der realen Welt als auch im Internet. Beim Treffen von solchen Vereinbarungen spielt die Unterschrift eine wichtige Rolle. Sie macht ein Dokument zu einer Urkunde. Urkunden genießen nach unserer Rechtsordnung die größte Beweiswürdigung im Fall eines Rechtsstreits. In Form von Kauf-, Verkaufs- oder Mietverträgen sind Urkunden die wichtigste Basis für eine (sichere) wirtschaftliche Betätigung. Gelingt es, die Funktionen, die die Unterschrift bei der Urkundenerstellung einnimmt (vgl. [7]), auch elektronisch als digitale Signatur nachzubilden, so ist dies ein wichtiger Schritt bei der Schaffung von Sicherheit beim Handel im Internet.

Funktionen der Unterschrift bei der Urkundenerstellung sind:

- **Identifikationsfunktion**
  Die Unterschrift gibt Auskunft über die Person des Unterzeichners.

- **Echtheitsfunktion**
  Das unterzeichnete Dokument lag dem Unterzeichner vor und wurde von ihm anerkannt.

- **Abschlußfunktion**
  Das unterzeichnete Dokument stellt eine abschließende Willenserklärung des Unterzeichners dar.

- **Warnfunktion**
  Durch die Notwendigkeit einer Unterschrift wird dem Unterzeichner verdeutlicht, daß ein rechtserheblicher Sachverhalt geschaffen wird.

Die Nachbildung der Funktionen der Unterschrift mit der digitalen Signatur kann aber nur in Verbindung mit einer gleichstellenden Verankerung in der Rechtssprechung auch dieselbe Rechtssicherheit wie Urkunden bieten. Dies ist für qualifizierte elektronische Signaturen nach dem Signaturgesetz (vgl. Abschnitt 5) der Fall (vgl. [18] und [20]). Die Beweiswürdigung anderer Arten der digitalen Signatur unterliegt dem Ermessensspielraum des Richters.

2.2. Funktionsweise

Die Funktionsweise von digitalen Signaturen basiert auf der speziellen Anwendung von Public-Key-Verfahren. Dabei muß der Tatsache Rechnung getragen werden, daß nur eine Person im Sinne der Authentifizierung ein Dokument unterschreiben/signieren darf, aber potentiell jeder diese Signatur überprüfen können muß. Dies erreicht man durch umgekehrte Anwendung eines Public-Key-Verfahrens.

Bei einem ersten Ansatz zur Realisierung einer digitalen Signatur verschlüsselt der Unterzeichner das zu signierende Dokument mit seinem privaten Schlüssel. Dieses Dokument kann von einer anderen Person nur mit dem zugehörigen öffentlichen Schlüssel wieder entschlüsselt werden. Die Tatsache, daß ein so verschlüsseltes Dokument durch den öffentlichen Schlüssel wieder in Klartextform dargestellt wird, sichert zu, daß das Dokument nicht manipuliert wurde, denn nur der Absender verfügt über den zur Verschlüsselung notwendigen zugehörigen privaten Schlüssel.

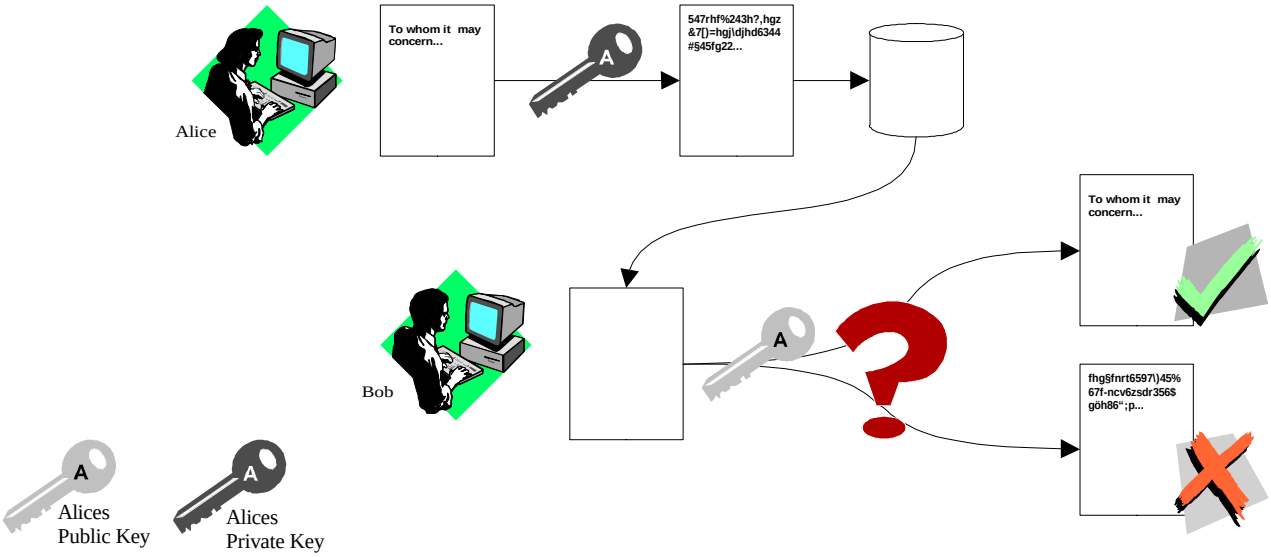

Abb. 4: Erster Ansatz zur digitalen Signatur

Wegen der Anwendung eines Public-Key-Verfahrens auf das vollständige zu unterzeichnende Dokument braucht dieser Ansatz wesentlich mehr Rechenzeit als der anschließende zweite Ansatz. Desweiteren wird die Abgrenzung von Dokument und Signatur, wie sie auch in der Realität vorherrscht, verwischt, da Dokument und Signatur hier eine Einheit bilden.

Statt, wie beim ersten Ansatz, das gesamte zu signierende Dokument zu verschlüsseln, berechnet man bei einer verbesserten zweiten Variante einen Hashwert fester Länge aus dem Dokument und verschlüsselt diesen anschließend. Die benutzte Hashfunktion muß bei der Änderung auch nur eines Bits des Ausgangsdokuments einen völlig anderen Hashwert liefern und es dürfen keine zwei

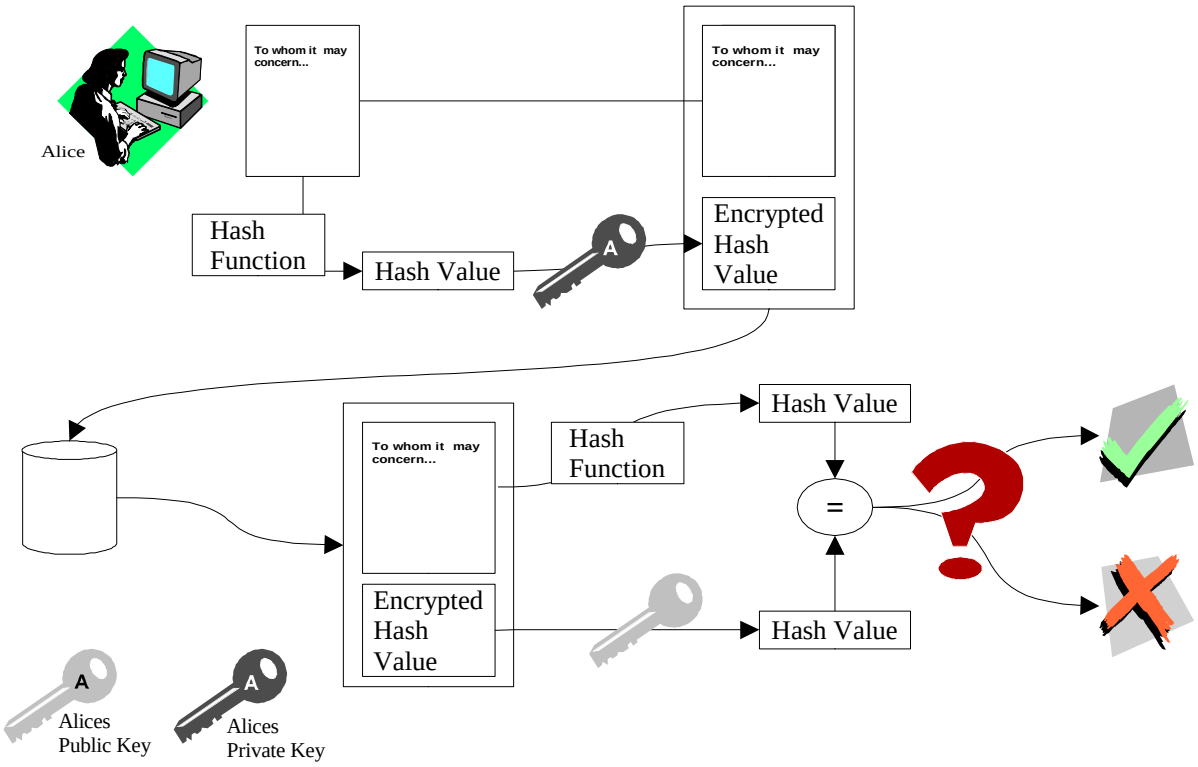

Abb. 5: Prinzip der digitalen Signatur

"sinnvollen" Dokumente den gleichen Hashwert liefern. Desweiteren darf kein Rückschluß vom Hashwert auf das ihn erzeugende Dokument möglich sein (Einweg-Hashfunktion). Diese hohen Anforderungen an die Hashfunktion erlauben es, anhand des Hashwertes unerlaubte Modifikationen am zu signierenden Dokument sicher zu erkennen.

Den mit dem privaten Schlüssel des Signierers verschlüsselten Hashwert nennt man dann die digitale Signatur dieses Dokuments. Sie wird an die unverschlüsselte Version des zu signierenden Dokuments angehängt.

Will eine andere Person die Integrität des Dokuments überprüfen, so berechnet sie aus der ihr vorliegenden Version des signierten Dokuments mit der gleichen Hash-Funktion wie der Signierer den zugehörigen Hashwert. Anschließend kann durch einen Vergleich mit dem aus der Signatur gewonnenen Hashwert festgestellt werden, ob Änderungen an dem Dokument vorgenommen wurden.

Der hier beschriebene zweite Ansatz wird in dieser Art bei den heutigen Formen der digitalen Sigantur angewendet. Auch PGP benutzt diesen zweiten Ansatz. Als Hash-Verfahren kommen dabei MD5 und SHA-1 zum Einsatz [10].

3. Digitale Zertifikate

3.1. Notwendigkeit und Bedeutung digitaler Zertifikate

Digitale Signaturen wie in Abschnitt 2.2. beschrieben können die Funktionen der Unterschrift aus Abschnitt 2.1. nicht vollständig erfüllen. Wie bereits in Abschnitt 1.3. bemängelt, läßt sich zu einem über einen unsicheren Kanal erhaltenen öffentlichen Schlüssel nicht zuverlässig auf die Identität des Eigentümers schließen. Denkbar ist hier z. B., daß ein Unbefugter den Schlüssel bei der Übermittlung durch seinen eigenen ersetzt. Er kann so alle Nachrichten bei der Kommunikation abfangen; leitet er die abgefangenen Nachrichten unter erneuter Verschlüsselung mit den entsprechenden öffentlichen Schlüsseln weiter, bemerken die Kommunikationspartner noch nicht einmal, daß sie abgehört werden. Dies ist neben dem in Abschnitt 1.2. beschriebenen Szenario eine weitere klassische Form eines Man-in-the-middle-Attack. Digitale Zertifikate bieten für das beschriebene Problem eine Lösungsmöglichkeit.

3.2. Aufbau und Funktionsweise

Ein digitales Zertifikat ist ein elektronisches Dokument, das durch eine digitale Signatur bescheinigt, daß der im Zertifikat enthaltene öffentliche Schlüssel an die Identität des Zertifikatinhabers gebunden ist. Die Funktion eines digitalen Zertifikates kann dabei mit der eines Personalausweises verglichen werden. Ohne ein digitales Zertifikat kann man nicht sicher sein, daß ein öffentlicher Schlüssel zu einer bestimmten Person gehört.

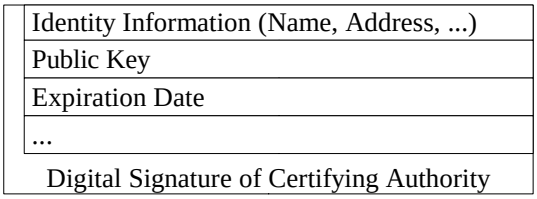

Abb. 6: Aufbau eines digitalen Zertifikats

Verfügt man über ein digitales Zertifikat einer anderen Person und will eine verschlüsselte Botschaft an diese schicken, so muß zunächst die Signatur des Zertifikats überprüft werden. Dazu ist es notwenig, daß man der Person, die das Zertifikat erstellt/unterschrieben hat, vertraut (Vertrauen bedeutet hier, daß Sicherheit über die Identität der Person sowie ihren zugehörigen öffentlichen Schlüssel besteht.). Ist dies der Fall, dann kann mit Hilfe des öffentlichen Schlüssels des Zertifizierers die Integrität des Zertifikats sicher überprüft und damit festgestellt werden, ob der im Zertifikat vermerkte öffentliche Schlüssel wirklich zu der angegebenen Person gehört.

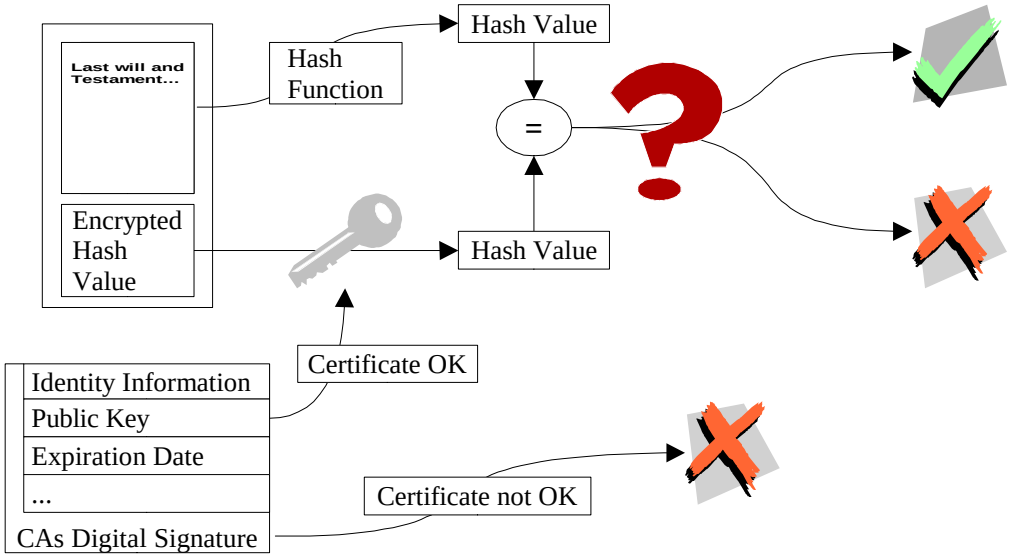

Abb. 7: Signaturprüfung unter Verwendung eines digitalen Zertifikats

Ein wichtiger Standard für den Aufbau digitaler Zertifikate, wie sie auch vom SSL-Protokoll benutzt werden, ist X.509, eine weitere wichtige Rolle spielen PGP-Zertifikate.

4. Trustmodelle (Sicherheitsinfrastrukturen)

Prinzipiell kann jeder ein digitales Zertifikat für eine andere Person erstellen. Dazu muß der Zertifikatsersteller (im folgenden CA = Certifying Authority genannt) zweifelsfrei feststellen können, daß die betreffende Person die ist, die sie zu sein vorgibt, sowie, daß ein entsprechender öffentlicher Schlüssel zu ihr gehört. Wegen der großen sicherheitsrelevanten Bedeutung des Zertifiziervorgangs ist es daher am besten, wenn die zu zertifizierende Person persönlich bei der CA erscheint und sich dort identifiziert sowie einen öffentlichen Schlüssel vorlegt.

Es ist möglich, daß CA's einer zweiten CA ein digitales Zertifikat erstellen. Alle Personen die der ersten CA vertrauen, vertrauen neben den dort zertifizierten Personen auch der zweiten CA und als Folge allen Personen, die bei der zweiten CA zertifiziert sind. Dieser Vorgang kann so fortgesetzt werden, und es ergeben sich verschiedene Szenarien der Zertifizierung, die man auch als Trustmodelle bezeichnet.

Direct Trust

Direct Trust ist das einfachste Trustmodell. In diesem Modell vertraut ein Benutzer dem öffentlichen Schlüssel eines anderen Benutzers, weil er ihn kennt und daher sicher ist, daß sein Schlüssel echt ist. Zertifikate spielen in diesem Modell keine Rolle.

Abb. 8: Direct Trust

Hierarchical Trust

Hierachical Trust liegt vor, wenn sich CA's in Ebenen einteilen lassen, so daß sich CA's einer Ebene ausschließlich bei einer CA einer höheren Ebene zertifizieren lassen. Es entstehen baumartige Strukturen von Zertifizierungsstellen. Dabei ist es lediglich notwendig, der Wurzelinstanz der Zertifizierungshierarchie zu vertrauen, um gleichzeitig allen Teilnehmern dieser Hierarchie zu vertrauen.

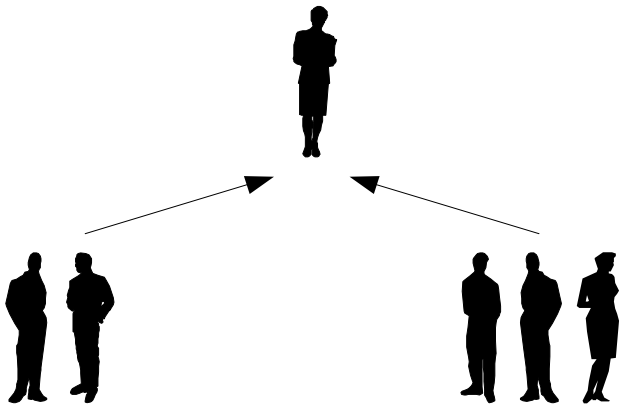

Abb. 9: Hierarchical Trust

Web of Trust

Gelten keine weiteren Einschränkungen für die CA's, so entsteht ein lose zusammenhängendes Netzwerk aus CA's. PGP benutzt dieses Trustmodell, und es wird wegen seiner Ähnlichkeit zum Aufbau des Internet auch Web of Trust genannt.

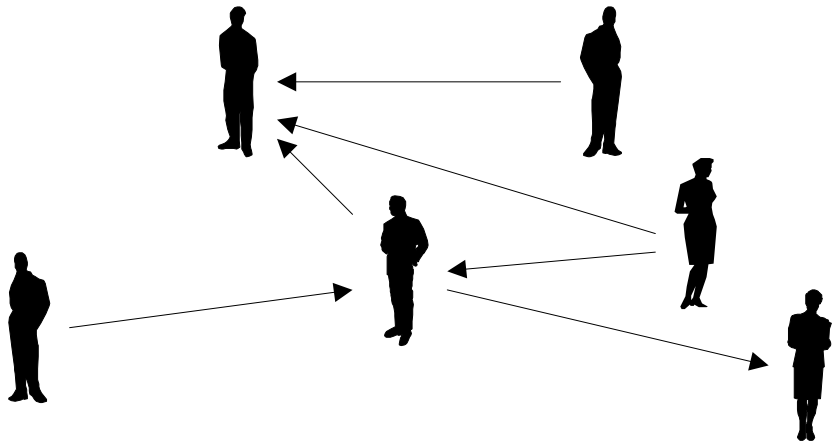

Abb. 10: Web of Trust

Die Problematik bei den beiden letztgenannten Trustmodellen ist, daß zu einem gegebenen Zertifikat ein möglichst kurzer Pfad zu einer CA gefunden werden muß, der man selbst vertraut (beim Hierarchical Trust ist dies i.d.R. die Wurzelinstanz). Dies liegt daran, daß mit der Länge des Pfades auch die Möglichkeit steigt, daß sich ein ungültiges Zertifikat im Pfad befindet.

Im Fall von PGP werden die Zertifikate auf öffentlich zugänglichen Servern abgelegt, die ständig weltweit abgeglichen werden, sodaß jeder PGP-Server sämtliche Zertifikate speichert. Spezielle Programme ermitteln dann bei Bedarf anhand der Zertifikate auf einem PGP-Server die kürzesten Pfade.

Beim Hierarchical Trust ist es von Vorteil, die Hierachie so flach wie möglich und damit die Pfade so kurz wie möglich zu halten.

Die Sicherheit der Trustmodelle kann man weiter steigern, wenn man nur speziell ausgestatteten und mit besonderen Auflagen auferlegten Einrichtungen das Ausstellen von Zertifikaten erlaubt, womit verhindert werden soll, daß falsche Zertifikate ausgestellt werden.

Zertifikate können aus verschiedenen Gründen ungültig werden. Dies ist zum Beispiel der Fall, wenn das im Zertifikat eingetragene Verfallsdatum (das i.d.R. zum Schutz vor krytographischen Attacken mitaufgenommen wird) überschritten wurde. Eine vorzeitige Invalidation des Zertifikats ist zum Beispiel möglich, wenn der entsprechende private Schlüssel ausgespäht wurde oder das Zertifikat für einen Mitarbeiter erstellt wurde, der die Firma verlassen hat. Im Falle einer vorzeitigen Invalidation muß diese der Öffentlichkeit mitgeteilt werden. Im Fall von PGP wird zu diesem Zweck auf den PGP-Servern eine Key-Revocation-List vorgehalten. Auch im Fall von Hierarchical Trust müssen die CA's solche Informationen bereitstellen.

5. Signaturgesetz (SigG) und Signaturverordnung (SigV)

5.1. Motivation

In Deutschland hat man die Bedeutung digitaler Signaturen bereits früh erkannt und bemerkt, daß ohne gesetzliche Regulierungen beim Aufbau einer Sicherheitsheitsinfrastruktur von rechtlicher Seite keine Sicherheit von digitalen Signaturen gewährleistet werden kann. Aus diesem Grund wurde am 1. August 1997 das Gesetz zur digitalen Signatur (SigG) als Artikel 3 des Informations- und Kommunikationsdienste Gesetzes (IuKDG) (auch bekannt als "Multimediagesetz") in Kraft gesetzt. Dieses Gesetz wurde am 22. Mai 2001 durch ein neues Signaturgesetz ersetzt, das die EU-Richtlinie

für „Gemeinsame Rahmenbedingungen für elektronische Signaturen“ vom 13. Dezember 1999 in national geltendes Recht umsetzt. Das Signaturgesetz soll die Rahmenbedingungen für elektronische Signaturen schaffen (§1 (1) SigG). Es regelt im wesentlichen die gesetzlichen Anforderungen an Zertifizierungsstellen sowie Anforderungen an elektronische (digitale) Signaturen.

5.2. Inhalt

Das Signaturgesetz sieht eine Einteilung digitaler Signaturen in drei Kategorien vor (§2, 2. SigG):

? elektronische Signaturen

? fortgeschrittene elektronische Signaturen

? qualifizierte elektronische Signaturen

Während die Anforderungen an digitale Signaturen der ersten Kategorie sehr niedrig sind („Daten (...), die zur Authentifizierung dienen“, §2, 1. SigG), müssen fortgeschrittene elektronische Signaturen spezielle Anforderungen erfüllen (im wesentlichen die Eigenschaften digitaler Signaturen, wie sie in Abschnitt 2 beschrieben werden). Eine fortgeschrittene elektronische Signatur wird als qualifizierte elektronische Signatur bezeichnet, wenn sie auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat (im Sinne des Signaturgesetzes) beruht und auf einer sicheren Signaturerstellungseinheit (z. B. Kryptprozessor) erzeugt wurde.

Zertifizierungsstellen unterliegen nach dem Signaturgesetz keiner Genehmigungspflicht, können sich aber freiwillig akkreditieren lassen, um sich im Rechts- und Geschäftsverkehr auf nachgewiesene Sicherheit berufen zu können (§15 (1) SigG). In jedem Fall ist die Zertifizierungsstelle verpflichtet, eine Deckungsvorsorge zu treffen, um für eventuelle Schäden durch mangelhafte elektronische Signaturen oder Zertifikate haften zu können (§12 SigG).

Nach §23 (1) SigG sind ausländische elektronische Signaturen qualifizierten elektronischen Signaturen gleichgestellt, sofern sie den Richtlinien in [3] entsprechen.

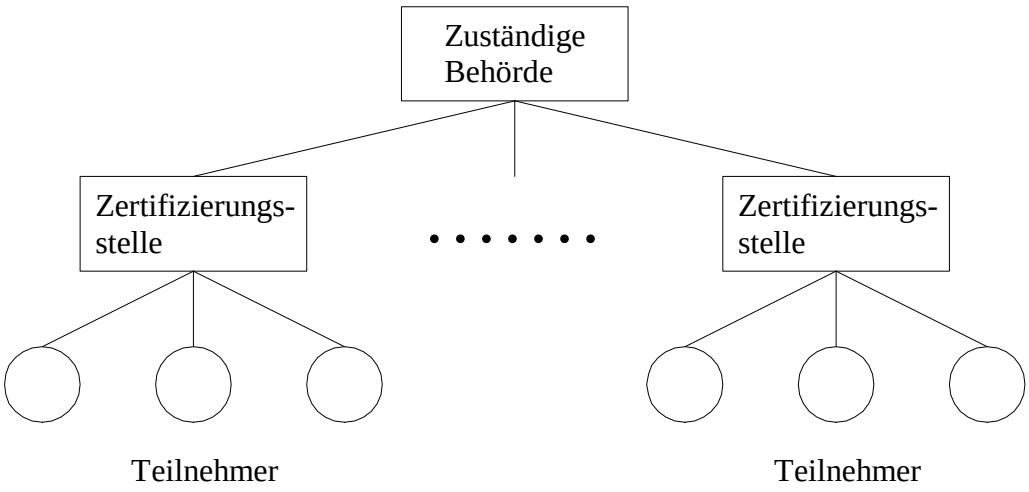

Abb. 11: Zertifizierungshierarchie nach dem Signaturgesetz

Das Signaturgesetz sieht, wie aus Abbildung 11 ersichtlich, eine zweistufige Sicherheitsinfrastruktur von Zertifizierungsstellen vor. Die Signaturverordnung (SigV) mit den zugehörigen

Maßnahmenkatalogen regelt die konkreten Vorschriften für die Zertifizierungsstellen zur Umsetzung des Signaturgesetzes. Für das aktuelle Signaturgesetz liegt momentan noch keine Signaturverordnung vor.

Die Signaturverordnung von 1997 legt die einzelnen Aufgaben innerhalb einer Zertifizierungsstelle und ihre Zusammenhänge wie folgt fest:

- **Schlüsselgenerierung / Key Generation**
  Es sind für die Zertifizierungsstelle und für Teilnehmer Schlüssel zu generieren.

- **Schlüsselzertifizierung / Certification Authority**
  Die Teilnehmerdaten, der korrespondierende öffentliche Schlüssel und weitere Daten werden zusammengefaßt und von der CA signiert.

- **Personalisierung / Personalization Service**
  Das Zertifikat und öffentlicher und privater Schlüssel werden auf eine Signaturkomponente (z. B. eine Chipkarte) übertragen.

- **Identifizierung und Registrierung / Registration Authority**
  Die Teilnehmer werden gegen Vorlage eines Ausweises identifiziert und registriert.

- **Verzeichnisdienst / Directory Service**
  Zertifikate werden in einem öffentlichen Verzeichnis abrufbar gehalten, wenn der Teilnehmer einer solchen Veröffentlichung nicht widerspricht. In jedem Fall muß der Verzeichnisdienst Auskunft darüber geben, ob ein Zertifikat gesperrt ist oder nicht.

- **Zeitstempeldienst / Time Stamping Service**
  Für bestimmte Daten kann es notwendig sein, diese mit einem vertrauenswürdigen Zeitpunkt zu verknüpfen. Dazu wird der Zeitpunkt an die Daten angehängt und das Ergebnis vom Zeitstempeldienst digital signiert.

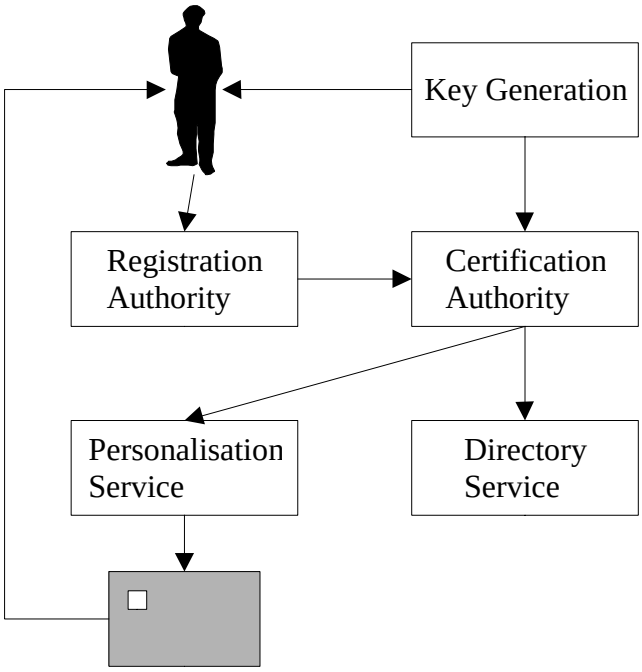

Abb. 12: Funktionaler Zusammenhang in einer Zertifizierungsstelle

5.3. Probleme und Mängel

Mit dem neuen Signaturgesetz vom 16.05.2001 ergeben sich neben den Vorteilen einer EU-weiten Regulierung des Einsatzes digitaler Signaturen aber auch eine Reihe von Nachteilen und Unklarheiten.

- **?** Während das Signaturgesetz von 1997 lediglich eine Art von digitalen Signaturen und digitalen Zertifikaten vorsah, beschreibt das Signaturgesetz vom 16.05.2001 drei Arten digitaler Signaturen. Dabei wird lediglich qualifizierten elektronischen Signaturen eine ähnliche Stelleung wie digitalen Signaturen nach dem Signaturgesetz von 1997 eingeräumt. Die verbleibenden beiden Arten digitaler Signaturen können nur eingeschränkte Rechtssicherheit bieten.

- **?** Zum Aufbau von Zertifizierungsstellen zur Ausgabe qualifizierter Zertifikate sind aufgrund der hohen Sicherheitsanforderungen erhebliche Investitionen notwendig, die letztlich direkt oder indirekt auf die Nutzer der Zertifizierungsstelle abgewälzt werden müssen.

- **?** Digitale Signaturen aus dem außereuropäischen Ausland, die nicht den Richtlinien in [3] genügen, bieten weiterhin geringe oder keine Rechtssicherheit. Dies stellt einen Nachteil für den Handel mit dem außereuropäischen Ausland dar.

Es bleibt also abzuwarten, inwiefern die genannten Punkte Einfluß auf den Einsatz und die Verbreitung digitaler Signaturen haben.

6. Zusammenfassung

Rechtliche Sicherheit im Internet spielt mit dessen Wachstum und der zunehmenden Nutzung des Internet für kommerzielle Zwecke eine stetig zunehmende Rolle. Ein Kernelement zur Verwirklichung der Rechtssicherheit im Internet spielt die digitale Signatur, die die Funktionen der eigenhändigen Unterschrift bei der Urkundenerstellung nachbilden soll. Zur Umsetzung der Funktionen der eigenhändigen Unterschrift in ein digitales Äquivalent bedient man sich dabei der Hilfe von kryptographischen Verfahren.

Die speziellen Eigenheiten der eingesetzten asymmetrischen Verfahren (Problem der sicheren Authentisierung) machen digitale Zertifikate notwendig. Um Sicherheit bei der Zertifikatserstellung zu bieten und um die digitalen Zertifikate effektiv und sicher öffentlich verfügbar zu machen bedarf es einer Sicherheitsinfrastruktur. Das Signaturgesetz von 1997 hat für eine solche Sicherheitsinfrastruktur erstmals in Deutschland gesetzliche Richtlinien geschaffen.

Die Neufassung des Signaturgesetzes vom 16.05.2001 setzt die EU-Richtlinie für digitale Signaturen in national geltendes Recht um. Das neue Signaturgesetz entspricht daher den europaweiten Vorgaben für digitale Signaturen.

Im Gegensatz zu den strengen Anforderungen des Signaturgesetzes von 1997 sieht das neue Signaturgesetz eine Abstufung in drei Kategorien digitaler Signaturen vor. Dabei sind an qualifizierte elektronische Signaturen die höchsten Anforderungen geknüpft. Sie bieten in Zukunft die gleiche Rechtssicherheit wie eigenhändige Unterschriften (vgl. [18] und [20]).

Literatur

[1] Gesetz zur digitalen Signatur (Signaturgesetz - SigG) vom 22.07.1997 als Artikel 3 des „Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG)“

[2] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, 16.05.2001
http://www.netlaw.de/gesetze/sigg.htm

[3] EU-Richtlinie 1999/93/EG „Gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“ vom 13.12.1999

[4] Lynch, D, Lundquist, L.: Digital Money - The New Era of Internet Commerce, John Wiley & Sons, Inc., 1996

[5] Gehring, R.: Digitale Signaturen. Linux-Magazin 08/1998

[6] Gehring, R.: Asymmetrisches. Linux-Magazin 10/1998

[7] Meinhold, M., Luckhardt, N.: Echtheits-Zertifikat - Digitale Signaturen mit beweiskräftigem Zeitstempel. c't 08/1998, S. 112 ff.

[8] Fox, D.: Automatische Autogramme - Mit digitalen Signaturen von der Datei zur Urkunde. c't 10/1995, S. 278 ff.

[9] Kryptocrew: Algorithmen. Juni 2001
http://www.kryptocrew.de/krypto/algo.html

[10] Network Associates, Inc.: An Introduction to Cryptography, 1999
ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf

[11] Bundesamt für Sicherheit in der Informationstechnik: Signaturgesetz und –verordnung - Die ersten Schritte, Stand 31.03.2000
http://www.bsi.de/aufgaben/projekte/pbdigsig/download/siswv.pdf

[12] Bundesamt für Sicherheit in der Informationstechnik: Digitale Signaturen, Stand 31.03.2000
http://www.bsi.de/aufgaben/projekte/pbdigsig/download/ds.pdf

[13] Bundesamt für Sicherheit in der Informationstechnik: Maßnahmenempfehlungen: Infrastruktur für Zertifizierungsstellen (SigG/SigV), Stand 31.03.2000
http://www.bsi.de/aufgaben/projekte/pbdigsig/download/tcinfra.pdf

[14] Bundesamt für Sicherheit in der Informationstechnik: Digitale Signatur nach dem deutschen Signaturgesetz, Stand 31.03.2000
http://www.bsi.de/aufgaben/projekte/pbdigsig/download/fbl_20.pdf

[15] TrustCenter GmbH: Die digitale Signatur - Rechtlicher Hintergrund, 18.04.2001
http://www.trustcenter.de/legal/back_info/de/dig_sig.htm

[16] TrustCenter GmbH: Allgemeine Informationen zur Verschlüsselungstechnik, 07.02.2001
http://www.trustcenter.de/legal/back_info/de/allgemein.htm

[17] TrustCenter GmbH: Sichere Internet-Kommunikation mit Zertifikat, 12.04.2001
http://www.trustcenter.de/infocenter/hintergrund-infos.htm

[18] Spiegel Online: Die elektronische Signatur ist Gesetz, 22.05.2001
http://www.spiegel.de/netzwelt/ebusiness/0,1518,135413,00.html

[19] Diering, M., Schmeh, K.: Zertifizierter Paragrafendschungel - Signaturgesetze in Europa, c't 13/2001 S. 182 ff.

[20] Bundesministerium für Wirtschaft und Technologie: Neues Signaturgesetz ab heute in Kraft - Wichtige Voraussetzungen für rechtsgültigen E-Commerce geschaffen, Pressemitteilung vom 22.05.2001
http://www.bmwi.de/Homepage/Presseforum/Pressemitteilungen/2001/1522prm2.jsp