Leibniz-Rechenzentrum München

Verschlüsselung im Internet*

Helmut Richter**

6.3.2002

Zusammenfassung

Im Zusammenhang mit der Sicherung des Datenverkehrs im Internet liest man Begriffe wie 'asymmetrische Verschlüsselung', 'Public-Key-Infrastruktur' oder 'Zertifikat'. In diesem Artikel werden diese Begriffe im Zusammenhang erläutert. Seine Lektüre wird denen empfohlen, die diese Techniken nicht nur anwenden, sondern auch verstehen wollen.

Inhaltsverzeichnis

*http://www.lrz-muenchen.de/services/security/pki/
**http://www.lrz-muenchen.de/persons/helmut_richter.html

1 Ziele der Verschlüsselung

Verschlüsselungstechniken im Internet dienen drei verschiedenen Zielen:

- **Vertraulichkeit**: Eine Nachricht nur für den lesbar zu machen, für den sie bestimmt ist, war von je her der Zweck von Geheimschriften und Verschlüsselungen.

- **Authentisierung**: Sicherzustellen, dass eine Nachricht wirklich von demjenigen stammt, dessen Name als Verfasser dabeisteht, wird gemeinhin *nicht* mit Geheimschriften und Verschlüsselungen assoziiert, sondern mit Unterschriften, Stempeln und Siegeln. Wir werden jedoch sehen, dass man Verschlüsselungstechniken auch zu diesem Zweck einsetzen kann. In diesem Zusammenhang spricht man dementsprechend von digitalen Signaturen.

  Diese *Authentisierung* (Überprüfung einer bestimmten Identität) darf nicht mit *Autorisierung* (Verleihung bestimmter Rechte und Zuständigkeiten) verwechselt werden. Im täglichen Leben wird manchmal beides gleichzeitig abgehandelt: so wird mit einem Dienstausweis, der ein Lichtbild enthält, gleichzeitig die Identität des Ausweisinhabers (Authentisierung) und seine Zugehörigkeit zu einer Gruppe mit bestimmten Rechten nachgewiesen (Autorisierung). Daneben gibt es reine Authentisierungsdokumente wie den Personalausweis und reine Autorisierungsdokumente wie Dienstausweise ohne Lichtbild, die nur gemeinsam mit einem Authentisierungsdokument gültig sind.

- **Unverfälschtheit**: Sicherzustellen, dass eine Nachricht auf dem Weg vom Absender zum Empfänger nicht verändert wird, ist eigenlich ein Spezialfall des voranstehenden Punktes, weil man Authentizitätsüberprüfungen mittels digitaler Signaturen auch zur Sicherung gegen Verfälschungen verwenden kann:

  – Ist es so, dass der Empfänger die Signatur des Absenders überprüfen kann, so ist die Aufgabe einfach: Digitale Signaturen hängen nämlich vom Text der gesamten Nachricht ab, so dass eine Verfälschung der Nachricht durch einen Übermittler dadurch bemerkt wird, dass sie wegen der nicht mehr passenden Signatur nicht mehr als authentisch betrachtet wird.

  – Oft ist diese Voraussetzung nicht erfüllt, dafür kann aber der Absender die Signatur des Empfängers überprüfen, z.B. wenn schutzwürdige Daten an einen WWW-basierten Dienst mit vielen Kunden gesandt werden. Dann kann man immer noch Unverfälschtheit garantieren, indem nach Authentisierung des Servers ein Schlüssel zur vertraulichen Kommunikation ausgetauscht wird. Wie diese Kombination von Authentisierung und Vertraulichkeit genau vor sich geht, wird weiter unten[1] erklärt.

Welche Verschlüsselungstechnik für einen bestimmten Zweck eingesetzt wird, richtet sich danach, welche dieser Ziele angestrebt werden. Außerdem kann es eine wichtige Rolle spielen, wie lange die Sicherheit aufrecht erhalten werden muss; darauf wird weiter unten[2] noch einmal eingegangen.

2 Methoden der Verschlüsselung

Eine konkrete Verschlüsselung besteht immer aus zwei Komponenten: einem *Verfahren* und einem *Schlüssel*. Das Verfahren legt fest, was zu tun ist. In einer sehr einfachen Verschlüsselung könnte etwa das Verfahren darin bestehen, dass jeder Buchstabenwert um eine feste Zahl erhöht wird; der

[1] siehe ☞ 2 auf Seite 6

[2] siehe ☞ 4 auf Seite 11

Schlüssel ist dann die zusätzliche Information dazu (hier etwa der Wert dieser festen Zahl). Das Verfahren ist allgemein bekannt; es wäre ja auch sehr schwierig, weltweit Verschlüsselungssoftware zu installieren und dabei geheimzuhalten, wie sie funktioniert; nur der Schlüssel wechselt von einem Anwender des Verfahrens zum nächsten und muss daher in der Regel geheimgehalten werden.

Die Entschlüsselung geht oft nach demselben Verfahren wie die Verschlüsselung vor sich, nur mit einem anderen Schlüssel.

Die Verschlüsselungsverfahren lassen sich danach einteilen, wer in der Lage ist, einen verschlüsselten Text wieder zu entschlüsseln. Für diese Unterscheidung muss man also wissen, ob es zu einem Schlüssel für die Verschlüsselung einen Schlüssel für die zugehörige Entschlüsselung gibt und ob sich der eine aus dem anderen ermitteln lässt und umgekehrt.

2.1 Ein-Weg-Verschlüsselung, "Fingerabdrücke"

Die Ein-Weg-Verschlüsselung ist eine echte Sackgasse: ist der Text einmal verschlüsselt, so kann ihn *niemand* mehr entschlüsseln. Diese Verfahren sind daher, wenn sie korrekt entworfen sind, sehr sicher, da es keinerlei Geheimnis über den Schlüssel gibt, das Unbefugten in die Hände fallen könnte. In der Regel können sogar verschiedene Klartexte zum selben verschlüsselten Text führen; manchmal macht man sich das zunutze, um den Text bei der Verschlüsselung zu kürzen.

Angewandt werden solche Verfahren, wo es nicht nötig ist, dass der Klartext zurückgewonnen werden kann:

- Passwörter werden in verschlüsselter Form gespeichert. Bei der Eingabe eines Passworts wird es mit demselben Verfahren verschlüsselt und mit dem gespeicherten verglichen. Es ist nicht nötig, das Passwort im Klartext zurückzugewinnen - im Gegenteil, es ist sehr erwünscht, dass das nicht geht. Was natürlich schon geht, ist, aus einer Liste von verschlüsselten Passwörtern diejenigen herauszufischen, die im Klartext einen von relativ wenigen vorgegebenen Werten haben, beispielsweise die in einem Wörterbuch stehen.

- Längere Texte werden mit einem solchen Verfahren auf einen wesentlich kürzeren "Fingerabdruck" komprimiert. Hängt dieser vom gesamten Text ab und ist lang genug, und ist das Verfahren sorgfältig entworfen, dann wird es nicht möglich sein, einen anderen Ausgangstext zu konstruieren, der nach Verschlüsselung genauso aussieht. Damit ist es möglich, die Unverfälschtheit einer Nachricht zu überprüfen, indem man *auf einem anderen Weg* gleichzeitig den Fingerabdruck übermittelt. Man kann beispielsweise bei der Ankündigung einer neuen Softwareversion deren Fingerabdruck mit bekanntgeben, den der Benutzer dann nach einem Download überprüfen kann.

In der englischsprachigen Literatur findet man für solche Verfahren die Begriffe *hash* und *digest*. Ersterer ist ein wenig unglücklich. Er stammt aus der Datenhaltung und bezeichnet die Komprimierung eines längeren Inhalts auf eine verkürzte Darstellung zum effizienteren Zugriff. Ein gutes Verfahren zur Ein-Weg-Verschlüsselung wird zwar in der Regel auch ein gutes Hash-Verfahren sein; das Umgekehrte gilt aber nicht: für ein Hash-Verfahren ist es gleichgültig, wie leicht man aus einem Hash-Wert einen Ausgangstext dazu konstruieren kann, während es für die Ein-Weg-Verschlüsselung ausschlaggebend ist, dass das nicht geht. Deswegen muss der von einer Ein-Weg-Verschlüsselung erzeugte Text auch eine gewisse Mindestlänge haben, um das Durchprobieren vieler Ausgangstexte unmöglich zu machen.

2.2 Symmetrische Verschlüsselung

Dies ist der Fall, an den man spontan denkt, wenn von Verschlüsselung die Rede ist: derjenige, der den Text verschlüsselt und derjenige, der ihn später entschlüsselt (das kann natürlich auch

derselbe sein, wenn die Verschlüsselung nur der sicheren Aufbewahrung dienen sollte), haben einen Schlüssel vereinbart, den sie beide benutzen. Wer verschlüsseln kann, kann auch entschlüsseln und umgekehrt. Das bedeutet in der Regel nicht, dass der Schlüssel zum Entschlüsseln exakt derselbe ist wie der zum Verschlüsseln - es reicht, wenn der eine in einfacher Weise aus dem anderen erschlossen werden kann.

Die Schwäche symmetrischer Verschlüsselungsverfahren in der Datenkommunikation ist die Notwendigkeit, zwischen Sender und Empfänger einer Nachricht den gemeinsam benutzten geheimen Schlüssel auszutauschen. Dieser Austausch darf nicht belauscht werden, sonst ist die gesamte Verschlüsselung zwecklos.

2.3 Asymmetrische Verschlüsselung

Die eben genannte Schwäche der symmetrischen Verschlüsselung wird bei der asymmetrischen Verschlüsselung vermieden. Hier reicht die Kenntnis der Verschlüsselung nicht zur Entschlüsselung aus und umgekehrt auch nicht. Das Verfahren selbst und der Schlüssel für eine Richtung darf daher ohne weiteres bekannt werden, wenn es für den Zweck der Anwendung ausreicht, dass der Schlüssel für die andere Richtung geheim bleibt.

Die Eigenschaft eines Textes, klar lesbar zu sein, ist zwar für den Nutzer des Textes interessant, nicht aber für die Verfahren zur Ver- und Entschlüsselung - für diese besteht kein Unterschied zwischen den beiden Richtungen. Es ist gleichgültig, ob ein Text zuerst ver- und dann entschlüsselt wird oder umgekehrt. Man kann sich das in einem Diagramm etwa so klarmachen:

einmal ent-	*verschlüsseln* Klartext	*verschlüsseln*	einmal ver-	*verschlüsseln*	zweimal
schlüssel-	——>	——>	schlüssel-	——>	ver-
ter Text	<——	<——	ter Text	<——	schlüssel-
	entschlüsseln	*entschlüsseln*		*entschlüsseln*	ter Text

Würde man nun hier die Begriffe "verschlüsseln" und "entschlüsseln" miteinander vertauschen, so läge ebenso eine voll verwendbare asymmetrische Verschlüsselung vor. Von dieser Vertauschbarkeit wird auch bei der Anwendung asymmetrischer Verschlüsselungstechniken Gebrauch gemacht. Die Begriffe "verschlüsseln" und "entschlüsseln" im obigen Diagramm sind sogar irreführend, weil keineswegs der eine Schlüssel zum Verschlüsseln (vom Klartext weg) und der andere zum Entschlüsseln (zum Klartext hin) verwendet wird. Vielmehr unterscheiden sich die beiden Schlüssel dadurch, wer sie verwenden soll und und durch die notwendige Geheimhaltung:

- Der *private Schlüssel* wird nur vom Eigentümer verwendet. Er darf auf keinen Fall anderen in die Hände fallen. Deswegen wird er *nie* aus der Hand gegeben, auch nicht zur Erstellung von Zertifikaten (was das ist, kommt weiter unten[3])

- Der *öffentliche Schlüssel* kann von jedermann im Verkehr mit dem Eigentümer verwendet werden. Deswegen darf er nicht nur jedermann bekannt sein, sondern soll es sogar.

Das Diagramm wird also sinnvoller mit diesen beiden Begriffen gebildet:

[3] siehe ☞ 3 auf Seite 8

privat verschlüsselter Text	*öffentl. Schlüssel anwenden* ——> <—— *privaten Schlüssel anwenden*	Klartext	*öffentl. Schlüssel anwenden* ——> <—— *privaten Schlüssel anwenden*	öffentl. verschlüsselter Text

Wir sehen uns nun an, wie die eingangs erwähnten drei Ziele mit Hilfe asymmetrischer Verfahren erreicht werden können. In diesen Erläuterungen wird "verschlüsseln" für die Richtung vom Klartext weg (also nach außen im Diagramm) und "entschlüsseln" für die Richtung zum Klartext hin verwendet.

- **Vertraulichkeit**: Um jemanden eine Nachricht so zukommen zu lassen, dass nur der Empfänger sie lesen kann, wird sie mit dem öffentlichen Schlüssel des Empfängers verschlüsselt, der ja allgemein bekannt ist. Der Empfänger entschlüsselt sie mit seinem privaten Schlüssel, den ja niemand kennt außer ihm selbst.

- **Authentisierung**: Um eine Nachricht unfälschbar mit ihrem Absender zu verbinden, wird sie mit dem privaten Schlüssel des Absenders verschlüsselt und dann werden *beide* Formen versandt. Der Empfänger kann die verschlüsselte Version mit dem öffentlichen Schlüssel des Absenders entschlüsseln und das Resultat mit der unverschlüsselten Nachricht vergleichen. Stimmen sie überein, so ist nachgewiesen, dass sie der Ansender selbst verschlüsselt hat, denn niemand sonst ist im Besitz des privaten Schlüssels. Die verschlüsselte Version wirkt also wie eine Unterschrift (Signatur) unter der unverschlüsselten Nachricht.

  Soll die Nachricht gleichzeitig signiert und vertraulich übertragen werden, lassen sich die Verfahren von diesem und vom voranstehenden Punkt auch gleichzeitig anwenden.

- **Unverfälschtheit**: Um sicherzustellen, dass eine Nachricht beim richtigen Empfänger unverfälscht ankommt, muss nicht unbedingt der Absender einen öffentlichen Schlüssel haben, der dem Empfänger bekannt ist (dann könnte der Absender ja einfach die Nachricht signieren). Es genügt auch, wenn der Absender, der selbst keinen öffentlichen Schlüssel zu haben braucht, den öffentlichen Schlüssel des Empfängers kennt. Dieser Fall tritt häufig dann ein, wenn der Empfänger ein von vielen Clients benutzter Server ist. Man geht dann so vor wie im Abschnitt über das SSL-Verfahren[4] erklärt.

Über diese drei eingangs erwähnten Einsatzzwecke hinaus lässt sich die Idee, die hinter den asymmetrischen Verschlüsselungen steckt, noch für einen vierten Zweck einsetzen, der hier nur interessehalber erwähnt wird, aber im Folgenden nicht mehr vorkommt:

- **Sichere Kommunikation ohne Schlüsselvereinbarung**: Bis jetzt musste man wenigstens den öffentlichen Schlüssel des Kommunikationspartners kennen, wollte man mit ihm über eine unsicheres Medium sicher kommunizieren. Es geht aber auch anders: zwei Kommunikationspartner denken sich jeweils eine Hälfte eines privaten Schlüssels aus und teilen sie dem anderen in einer solchen Weise verschlüsselt mit, dass man mit der *unverschlüsselten* anderen Hälfte einen ganzen Schlüssel zurückgewinnen kann. Dieses Verfahren von Diffie und Hellman[5] hat mit der asymmetrischen Verschlüsselung die Idee gemeinsam, dass es eine zahlentheoretische Funktion gibt, die in einer Richtung einfach und in der anderen undurchführbar komplex ist. Leider muss man bei seiner Anwendung auf die gleichzeitige Authentisierung des Kommunikationspartners verzichten, da die Pointe ja gerade darin besteht, dass die beiden Kommunikationspartner nichts vorab voneinander zu wissen brauchen.

[4] siehe ☜ 2 auf Seite 6

[5] `http://www.rsasecurity.com/rsalabs/faq/3-6-1.html`

2.4 Hybridverfahren

Wie man sieht, kann man mit asymmetrischen Verschlüsselungsverfahren alle drei Ziele erreichen. Der Aufwand für die Ver- und Entschlüsselung ist aber bei asymmetrischen Verfahren generell höher als bei symmetrischen, so dass man letztere dort verwendet, wo von der Asymmetrie gar kein Gebrauch gemacht wird. In der Praxis werden Ein-Weg-, symmetrische und asymmetrische Verfahren miteinander kombiniert eingesetzt:

- Eine Nachricht kann vertraulich übermittelt werden, indem man einen beliebigen zufälligen symmetrischen Schlüssel nur für dieses eine Mal generiert, diesen (symmetrischen) Schlüssel mit dem öffentlichen (asymmetrischen) Schlüssel des Empfängers verschlüsselt überträgt und die restliche Nachricht symmetrisch verschlüsselt. Mit anderen Worten: der asymmetrische Schlüssel sichert nicht die Nachricht, sondern den Austausch des symmetrischen Schlüssels. Da die Verletzlichkeit dieses Austauschs des wesentliche Schwachpunkt symmetrischer Verfahren ist, kann deren höhere Geschwindigkeit ohne Sicherheitseinbuße genutzt werden.

- Ein Spezialfall davon ist die Vereinbarung eines Sitzungsschlüssels im SSL-Verfahren wie unten beschrieben. Hier wird ebenfalls das aufwendigere asymmetrische Verfahren nur solange verwendet, wie seine Vorteile auch tatsächlich genutzt werden.

- Bei der digitalen Signatur (siehe im vorangegangenen Abschnitt unter "Authentisierung") muss nicht der gesamte Text veschlüsselt werden. Stattdessen wird der Text zuerst mit einem Ein-Weg-Verfahren auf einen Fingerabdruck gekürzt und nur der mit dem symmetrischen Schlüssel verschlüsselt. Da der Fingerabdruck vom gesamten Ausgangstext abhängt, würde eine Änderung an diesem die Signatur ungültig machen.

2.5 Beispiel: Secure Sockets Layer (SSL)


2

Der Verkehr im Internet ist durch sogenannte *Protokolle* geregelt. Dieses Wort hat hier nicht die Bedeutung "Niederschrift des Verlaufs von etwas", sondern "Regeln für die Abwicklung und die dabei zu verwendende Sprache", also dieselbe wie im täglichen Leben "diplomatisches Protokoll", "protokollarisch". Beispielsweise erfolgt der Zugriff eines WWW-Browsers auf die von einem WWW-Server angebotenen Daten über das HTTP-Protokoll, deswegen fängt die zum Zugriff benutzte Adresse, der URL, mit "http:" an.

Secure Sockets Layer (SSL) ist ein Verfahren, mit dem die Kommunikation über ein Internet-Protokoll zusätzlich verschlüsselt, signiert und authentisiert werden kann. Das zugrundeliegende Protokoll wird dabei nicht verändert. Wird etwa SSL beim Zugriff auf WWW-Seiten verwendet, dann werden genau dieselben Elemente des HTTP-Protokolls verwendet, mit denen man auch sonst auf einen WWW-Server zugreift, nur wird zusätzlich der gesamte Verkehr verschlüsselt; der Protokollname "https" statt "http", der am Anfang des URL steht, bezeichnet also nicht ein anderes Protokoll, sondern die zusätzliche Verschlüsselung.

Im SSL-Protokoll wird von Zertifikaten Gebrauch gemacht. Dieser Begriff wird erst im nächsten Kapitel[6] eingeführt. Zum Verständnis reicht es hier aus zu wissen, dass ein Zertifikat ein digitales Dokument ist, das einen öffentlichen Schlüssel einem Namen (einer Person oder einer Sache) zuordnet und dessen Richtigkeit überprüft werden kann.

SSL wird hier als Beispiel dafür benutzt, wie die verschiedenen Verschlüsselungsarten ineinandergreifen. Die folgende Darstellung des Ablaufs ist stark vereinfacht:

1. Der Client nimmt Kontakt zum Server auf und teilt unverschlüsselt mit, welche symmetrischen Verschlüsselungsverfahren er kennt und benutzen möchte.

[6] siehe 3 auf Seite 8

2. Der Server antwortet unverschlüsselt, welches dieser Verfahren davon im Folgenden verwendet werden soll. Er legt außerdem sein eigenes Zertifikat vor, damit der Client seine Identität überprüfen kann. Wenn umgekehrt auch der Server die Identität des Clients überprüfen will, kann er ein Zertifikat mit dem Schlüssel des Clients anfordern; das ist jedoch der weitaus seltenere Fall.

3. Der Client überprüft, ob das Zertifikat des Servers auf den Kommunikationspartner ausgestellt ist. Im Falle eines WWW-Servers muss das Zertifikat etwa auf eine Menge von URLs ausgestellt sein, unter denen sich die befindet, auf die im Anschluss zugegriffen werden soll.

4. Der Client generiert einen "Hauptschlüssel" und übermittelt ihn an den Server, und zwar mit dessen öffentlichem Schlüssel verschlüsselt, den er dem Zertifikat des Servers entnommen hat. Nur der authentische Server, dem der URL tatsächlich zugeordnet ist, wird daraus den Hauptschlüssel wieder zurückgewinnen können.

5. Hat der Server ein Zertifikat vom Client angefordert, sendet es der Client unverschlüsselt. Außerdem sendet er einen mit seinem privaten Schlüssel verschlüsselten Text zum Beweis, dass er im Besitz des privaten Schlüssels ist, der zum öffentlichen Schlüssel aus seinem Zertifikat passt. Der Text vor der Verschlüsselung ergibt sich aus dem bisherigen Verlauf der Kommunikation zwischen Server und Client, ist also nicht vom Client frei wählbar.

6. Beide Kommunikationspartner besitzen jetzt denselben Hauptschlüssel, den sonst niemand kennt, selbst wenn die bisherige Kommunikation belauscht wurde. Sie generieren jetzt beide aus dem Hauptschlüssel einen für das gemeinsam ausgewählte symmetrische Verschlüsselungsverfahren geeigneten Schlüssel und benutzen ihn von da an beide für die gesamte folgende Kommunikation.

Hier kommen also alle oben genannten Kombinationen verschiedener Verschlüsselungsverfahren zum Einsatz: symmetrische und asymmetrische wie eben beschrieben und Ein-Weg-Verfahren im Zusammenhang mit Signaturen.

2.6 Schlüssellängen

Je länger der Schlüssel ist, desto mehr mögliche Kombinationen gibt es und desto länger braucht man, um alle auszuprobieren. Das ist bei einem mechanischen Schlüssel nicht anders als bei einem kryptographischen; nur wird im einen Fall die Länge in Millimeter oder in "Zuhaltungen" gemessen und im andern Fall in Bits. Welche Schlüssellängen sind nun als sicher zu betrachten?

Man liest gelegentlich, dass asymmetrische Verfahren wesentlich größere Schlüssellängen benötigen als symmetrische. Der Grund dafür ist aber nicht, dass sie etwa bei gleicher Schlüssellänge unsicherer wären, sondern dass die Bedeutung des Wortes "sicher" in beiden Fällen verschieden ist:

- Man betrachtet eine symmetrische Verschlüsselung als sicher, wenn man aus dem verschlüsselten Text bei *unbekanntem* Schlüssel den Klartext nicht ermitteln kann und wenn man aus beliebig vielen Paaren von Klartext und zugehörigem verschlüsselten Text den Schlüssel nicht ermitteln kann.

- Man betrachtet eine asymmetrische Verschlüsselung als sicher, wenn sie es im ebengenannten Sinne ist und man außerdem selbst bei *bekanntem* Schlüssel für eine Richtung keine Ver- bzw. Entschlüsselung in der Gegenrichtung vornehmen kann.

Die Anforderungen an asymmetrische Verfahren sind also wesentlich höher; insbesondere ist ein symmetrisches Verfahren überhaupt nicht im zweiten Sinne sicher zu bekommen. Bei asymmetrischen Verfahren besteht ein mathematischer Zusammenhang zwischen Nachricht, öffentlichem und privatem Schlüssel, so dass der Schlüssel nicht durch Probieren, sondern durch systematisches Rechnen geknackt werden kann. Deswegen sind die Schlüssellängen nicht vergleichbar.

Diese Betrachtungen schließen nicht aus, dass es auch unter den asymmetrischen Verfahren solche gibt, die mit kürzeren Schlüsseln auskommen als andere, wenn nämlich der benutzbare mathematische Zusammenhang schwerer für einen effizienten Algorithmus ausnutzbar ist.

Als sicher gilt zur Zeit und wohl noch für eine ganze Weile eine Schlüssellänge von 128 Bit für symmetrische und von 2048 Bit für das asymmetrische RSA-Verfahren; andere asymmetrische Verfahren kommen zum Teil mit kürzeren Schlüssellängen aus. Weitere Details, die aber zum Verständnis hier nicht gebraucht werden, kann man in der Kryptographie-FAQ der Firma RSA[7] nachlesen.

3 Zertifikate


3

Überall wo asymmetrische Verschlüsselung eingesetzt wird, muss der öffentliche Schlüssel des Kommunikationspartners bekannt sein. Geht es dabei nur um die Sicherung der Vertraulichkeit, wird ein unbekannter oder falscher öffentlicher Schlüssel nur die vertrauliche Kommunikation sabotieren, was aber sofort bemerkt wird.

Anders ist es, wenn die asymmetrische Verschlüsselung einen Kommunikationspartner authentisieren soll, also in den Fällen, die oben unter "Authentisierung" (nämlich des Absenders) und unter "Unverfälschtheit" (d.h. Authentisierung des Empfängers) stehen. In diesen Fällen wirkt ein falscher oder unbekannter Schlüssel wie eine falsche Unterschrift, der man zu Unrecht vertraut, beziehungsweise wie eine unbekannte Unterschrift, die man nicht überprüfen kann.

Im täglichen Leben gibt es drei Mechanismen, den Zusammenhang zwischen einer Person und ihrer Unterschrift glaubwürdig herzustellen:

- **Beglaubigung**: Es gibt ein Dokument, das diesen Zusammenhang bescheinigt und dessen Echtheit leichter verifiziert werden kann als die der Unterschrift selbst. Es kann sich dabei um eine besondere Beglaubigung einer Unterschrift durch einen Notar oder eine Behörde handeln oder auch um ein schwer fälschbares Authentisierungsdokument wie einen Personalausweis. Beglaubigung allein kann natürlich nicht der einzige Verifikationsmechanismus sein, da jedes Beglaubigungsdokument ja selbst wieder beglaubigt werden müsste.

- **Öffentlichkeit**: Der Zusammenhang wird öffentlich bekanntgemacht und es wird darauf vertraut, dass eine falsche Unterschrift rechtzeitig auffallen würde. Ein Beispiel dafür ist etwa der Aushang der Unterschriften der zeichnungsberechtigten Mitarbeiter einer Bank in deren Geschäftsräumen. Aber in einem gewissen Sinn wird auch ein Personalausweis in dieser Weise bestätigt: die Echtheit des Personalausweises wird ja nicht durch Beglaubigung gewährleistet, sondern dadurch, dass sein Aussehen öffentlich bekannt ist - einem fremdländischen Ausweis, von dem man noch nie einen sicher echten zum Vergleich gesehen hat, würde man weit weniger vertrauen.

- **Persönliche Bekanntheit**: Ist der Geschäftsverkehr unter Umständen zustande gekommen, die es sehr wahrscheinlich erscheinen lassen, dass die beteiligten Personen die sind, die sie zu sein vorgeben, wird man auf Beglaubigungen der Unterschriften verzichten. Das ist in der Praxis der weitaus häufigste Fall.

[7] `http://www.rsasecurity.com/rsalabs/faq/`

Genau dieselben drei Mechanismen werden auch verwendet, um Schlüssel für die asymmetrische Verschlüsselung glaubwürding mit ihren Inhabern zu verbinden:

- **Beglaubigung**: Zusammen mit einem signierten Dokument wird ein weiteres, ebenfalls elektronisch signiertes Dokument vorgelegt, das die Signatur des ersten beglaubigt. Weil eine solche Beglaubigung auf englisch "certificate" heißt, wird sie auch im Deutschen meist als *Zertifikat* bezeichnet.

- **Öffentlichkeit**: Öffentliche Schlüssel werden öffentlich bekanntgemacht (z.B. mit ihren Fingerabdrücken[8] auf WWW-Seiten usw.) und es wird darauf vertraut, dass ein Fälscher die zahlreichen Veröffentlichungswege nicht gleichzeitig kompromittieren kann. Voraussetzung ist allerdings, dass sich die Nutzer tatsächlich den Schlüssel auf verschiedenen Wegen besorgen und vergleichen, was oft eine unrealistische Annahme ist.

- **Persönliche Bekanntheit**: Natürlich kann man einen Schlüssel, der im Verkehr zwischen wenigen Beteiligten verwendet wird, auch direkt unter den Beteiligten austauschen, indem man sich trifft oder indem man nach einem Versand der Schlüssel über das Internet die Fingerabdrücke[9] der Schlüssel telefonisch verifiziert.

Der Begriff "Zertifikat" wird oft falsch gebraucht. Wie jede andere Beglaubigung enthält ein Zertifikat nur öffentliche Information, nämlich die Verbindung eines öffentlichen Schlüssels mit dem Namen seines Eigentümers. Damit kann ein Zertifikat auf keinen Fall zu irgendetwas berechtigen. Der oft gehörte Ausdruck, eine Person oder eine Software-Instanz (z.B. ein WWW-Server) weise sich durch ihr Zertifikat aus, bedeutet also nicht, dass der *Besitz* des Zertifikats sie identifiziert. Vielmehr identifiziert sie der Besitz des privaten Schlüssels, der zu dem im Zertifikat beglaubigten öffentlichen Schlüssel passt.

Zertifikate spielen im abgesicherten Internet-Verkehr eine viel größere Rolle als Beglaubigungen im täglichen Leben. Das liegt daran, dass die Voraussetzungen für eine wirksame Kontrolle durch Öffentlichkeit oder durch persönliche Bekanntheit viel seltener gegeben sind. Es stellt sich daher die Frage, wo die Zertifizierungskette endet und welche Mechanismen dann greifen. Da nur endlich viele mögliche Zertifizierungsinstanzen in Frage kommen, muss nämlich jede Kette von Zertifikaten so enden, dass ein Zertifikat entweder vom Zertifikatsnehmer selbst unterzeichnet ist, oder aber auf einen Unterzeichner verweist, der selbst in der Kette schon vorkam. Hier gibt es zwei Modelle:

- **Zertifizierungshierarchie**: Es gibt eine Hierarchie, in der die höhere Instanz jeweils die Zertifikate für die niedrigere ausstellt. An der Spitze der Hierarchie stehen relativ wenige Wurzelinstanzen, deren Zertifikate man nicht durch Beglaubigungen überprüfen kann und die deswegen durch geeignete Maßnahmen für die überprüfbare Verbreitung ihrer öffentlichen Schlüssel sorgen müssen.

- **Vertrauensnetz**: Jeder Teilnehmer zertifiziert die Schlüssel derjenigen Teilnehmer, denen er vertraut und deren Schlüssel er überprüfen kann. Dadurch entsteht ein Netz gegenseitigen Vertrauens ähnlich der Situation, dass man einer Person vertraut, die einem von einem Freund als vertrauenswürdig vorgestellt wurde. Mit zunehmendem Abstand, d.h. mit zunehmender Anzahl von Mittelspersonen werden dann die Zertifikate als immer weniger vertrauenswürdig betrachtet.

Die beiden Modelle können auch nebeneinander existieren, wenn sich im ersten Modell Wurzelinstanzen gegenseitig zertifizieren (sog. Kreuzzertifizierung) oder wenn sich jemand seinen Schlüssel von mehreren unabhängigen Instanzen zertifizieren lässt. Im Folgenden wird stärker auf das erste Modell eingegangen.

[8] siehe ☜ 1 auf Seite 3

[9] siehe ☜ 1 auf Seite 3

3.1 Public-Key-Infrastrukturen

Unter einer Public-Key-Infrastruktur versteht man das, was nötig ist, um sinnvoll Zertifikate ausstellen zu können. Dazu gehört ein Satz Regeln, für welche Personen oder Instanzen Zertifikate ausgestellt werden und unter welchen Bedingungen, die Überprüfung der Identität der Zertifikatnehmer, meist auch die Veröffentlichung der ausgestellten und gegebenenfalls auch der widerrufenen Zertifikate, sowie vor allem geeignete Methoden, Zertifikate so zu erstellen, dass sie selbst vertrauenswürdig sind; insbesondere darf dazu der signierende Rechner in aller Regel nicht über das Internet erreichbar sein.

In vielen Fällen wird die Identitätsüberprüfung von der eigentlichen Zertifikatserstellung getrennt; dann wird zwischen der Registrierungsstelle (*registration authority*, RA) und der Zertifizierungsstelle (*certification authority*, CA) unterschieden. Im Sinne der Zertifizierungshierarchie kann auch eine Zertifizierungsstelle Zertifikate für eine andere Zertifizierungsstelle ausstellen.

Im täglichen Leben ist es einerseits jedermann unbenommen, sich von der Identität einer Person selbst zu überzeugen oder für andere eine Identitätsprüfung vorzunehmen, andererseits gibt es aber Einrichtungen wie Notariate oder Konsulate, die für diese Aufgabe besondere Verantwortung tragen. Ähnlich ist es bei Zertifikaten über elektronische Signaturen, die für eigene Zwecke oder im Verkehr im gegenseitigen Einvernehmen jeder erstellen kann. Sollen sie aber eine gewisse Rechtsverbindlichkeit erlangen, muss sich der Zertifizierungsdiensteanbieter an die Vorgaben des Signaturgesetzes[10] halten, zu denen neben Fachkunde, Sorgfalt und Dokumentation auch die Hinterlegung einer Deckungsvorsorge von 250.000 EUR für eventuelle Haftungsfälle gehört. Ist all das der Fall, so heißen die Zertifikate "qualifiziert". Das LRZ und ähnliche Institutionen stellen keine qualifizierten Zertifikate aus.

3.2 Zertifizierungshierarchien

Im Grunde kann eine Zertifizierungskette an jeder beliebigen Stelle mit einem selbstsignierten Zertifikat enden, also mit einem Zertifikat, das der Zertifikatnehmer selbst unterzeichnet hat. Derjenige, der dieses sogenannte Wurzelzertifikat überprüfen will, kann dann noch feststellen, dass der Unterzeichner selbst im Besitz des zugehörigen privaten Schlüssels ist; seine Identität kann er aber mit den Mitteln der Zertifizierung allein nicht mehr überprüfen. Hier sind ein paar Beispielfälle, wie es dann weitergeht:

- Der Unterzeichner ist eine bekannte Firma, die als Wurzel-CA auftritt. Dann besorgt man sich einmal deren Zertifikat, etwa über ihre WWW-Seite. Je nach persönlichem Misstrauen in die Sicherheit dieser WWW-Kommunikation kann man dann noch versuchen, den Fingerabdruck[11] unabhängig zu verifizieren: durch einen Anruf oder ein Anschreiben an diese Firma. Hat man das einmal hinter sich gebracht, hebt man das Zertifikat auf und hat Ruhe, solange das Zertifikat gültig ist.

  Um den Prozess zu vereinfachen, liefern Browser-Hersteller die Zertifikate einer Reihe solcher Firmen gleich mit. Meist ist das eine Vereinfachung; es kann aber auch ein zusätzliches Risiko[12] darstellen, weil dem Endbenutzer die Kontrolle darüber entzogen wird, dem er vertrauen will.

- Der Unterzeichner ist nicht so bekannt, spielt aber im lokalen Kontext des Endbenutzers eine Rolle. Dann geht man einfach genauso vor: man kann für sich selbst jeden Beliebigen als Unterzeichner eines Wurzelzertifikats akzeptieren.

[10] `http://www.netlaw.de/gesetze/sigg.htm`

[11] siehe ☜ 1 auf Seite 3

[12] siehe ☜ 5 auf Seite 13

- Ist das Zertifikat nur zum Testen ausgestellt, endet die Zertifikatkette meist rasch. Solange man genau die Tests durchführt, für die das Zertifikat ausgestellt wurde, darf man es akzeptieren, muss aber die Akzeptanz danach sofort rückgängig machen. Wenn man dafür sorgt, dass die vorübergehendende Akzeptanz keine Nebenwirkungen hat (im Wesentlichen dadurch, dass man solange keine anderen Applikationen startet, die Zertifikate überprüfen), braucht man das Testzertifikat überhaupt nicht zu überprüfen.

Zusammenfassend lässt sich also sagen: dort wo die Zertifikatkette endet, muss man selbst darüber entscheiden, ob man Vertrauen investieren will. Vertraut man einer großen Wurzelinstanz, so bekommt man danach keine Anfragen mehr aus dem gesamten Baum von Zertifizierungsstellen, an dessen Spitze diese Wurzelinstanz steht. Das ist bequem, aber man hat die Kontrolle, wem man vertrauen will, an diese Wurzelinstanz abgegeben.

Für die Hochschullandschaft Deutschlands gibt es zwei besonders herausragende Wurzelinstanzen:

- Die DFN-PCA[13] stellt Zertifikate für Zertifizierungsstellen in Hochschulrechenzentren aus. Das LRZ ist derzeit noch nicht dort zertifiziert; das soll aber Anfang 2002 erfolgen. Weder das Wurzelzertifikat noch die Zertifikate der einzelnen Zertifizierungsstellen sind qualifizierte Zertifikate im Sinne des Signaturgesetzes.

- Die Regulierungsbehörde für Telekommunikation und Post (RegTP)[14] ist Wurzelinstanz für die akkreditierten Zertifizierungsdiensteanbieter, die in Deutschland qualifizierte Zertifikate anbieten. Die Fingerabdrücke[15] der RegTP-Wurzelzertifikate sind im Bundesanzeiger veröffentlicht, so dass man sie im konkreten Fall überprüfen kann, wenn sie einem vorliegen. Über das Netz zugreifbar sind die Zertifikate praktisch nicht. (Man kann sie in einem proprietären Format herunterladen, zu dessen Interpretation man ein unbekanntes Programm installieren muss, wobei bei der Installation, die auch nur auf dem proprietären Betriebssystem eines einzigen Herstellers funktioniert, unbekannte Systemänderungen eingespielt werden müssen. Wer solches tut, ist wohl ohnehin der Falsche für Sicherheitsfragen.)

4 Das schwächste Glied der Kette

Bei der Diskussion der Frage, wie sicher die Kommunikation über das Internet durch Einsatz von Verschlüsselungtechniken ist, werden gerne Betrachtungen darüber angestellt, wie viel Rechenzeit notwendig ist, um bei gegebener Schlüssellänge den Code zu knacken. Solche Betrachtungen sind jedoch genauso irrelevant wie Betrachtungen über die Dicke einer Panzertür wenn daneben die Fenster des Gebäudes offen stehen. Eine Kette ist immer nur so stark wie ihr schwächstes Glied, und die Verschlüsselung ist schon bei schwachen Schlüssellängen (64 Bit symmetrisch, 1024 Bit asymmetrisch) ein relativ starkes Glied der Kette und bei vernünftigen Schlüssellängen (128 bzw. 2048 Bit) erst recht. Fast immer lauert die Gefahr woanders.

☞ 4

Bevor wir solche Gefahren im Einzelnen betrachten, sehen wir uns die Bedingungen an, unter denen sie auftreten:

- **Dauer des Schutzes**: Ein übertragenes Passwort braucht nur bis zur nächsten Passwortänderung geheim zu bleiben; ein übermittelter Code, mit dem andere Dokumente verschlüsselt wurden, muss so lange geheim bleiben, bis das letzte der damit verschlüsselten Dokumente nicht mehr der Geheimhaltung unterliegt; und die digitale Signatur unter einem Vertrag muss so lange sicher sein, wie eine Vertragspartei Rechte aus dem Vertrag geltend machen kann.

[13] `http://www.dfn-pca.de/certification/cacert.html`
[14] `http://www.nrca-ds.de`
[15] siehe ☞ 1 auf Seite 3

Besonders kurz ist die Dauer des notwendigen Schutzes, wenn es überhaupt nicht auf Geheimhaltung, sondern allein auf Authentisierung und Schutz vor Verfälschung ankommt. In diesen Fällen stört es nicht einmal, wenn kurz nach dem Ende der Sitzung die Schlüssel bekannt werden, mit denen diese Sitzung geschützt wurde.

Da Schutzmaßnahmen umso leichter zu planen sind, je kürzer der Zeitraum ist, für den sie Schutz gewähren müssen, ist es sinnvoll, an möglichst vielen Stellen zeitliche Beschränkungen der Gültigkeit von Schlüsseln und Dokumenten einzufügen. Allerdings widerspricht eine solche Begrenzung oft dem Zweck des Dokuments, beispielsweise bei langfristig gültigen Verträgen.

- **Motivation des Angreifers**: Hat ein möglicher Angreifer ein bestimmtes Ziel, etwa Industriespionage in einem bestimmten Unternehmen, so wird er andere Mittel einsetzen als jemand, der in einem Kommunikationsnetz die vorbeifließenden Daten nach *irgendwelchen* Informationen absucht, die ihm vielleicht nützlich sein können, wie etwa nach Passwörtern.

- **Höhe des Schadens**: Die Schutzmaßnahmen müssen sich in ihrem Aufwand natürlich auch danach richten, welcher Schaden entsteht, wenn sie überwunden werden: Wird "nur" die Privatsphäre verletzt, ohne dass klar ist, wer mit der Information etwas anfangen kann; werden betriebswichtige vertrauliche Daten preisgegeben; können Systeme manipuliert werden; werden Einfallstore für künftige Manipulationen geschaffen? Besonders unübersehbar sind die Folgen, wenn ein Schlüssel bekannt wird, mit dem Dokumente signiert werden; dann können beliebig neue Dokumente mit Datum auch in der Vergangenheit erstellt werden und es ist sehr schwierig, im Nachhinein die echten von den falschen zu unterscheiden.

4.1 Nichttechnische Gefahren

Nicht immer kommt die Gefahr aus dem Internet. Die Liste der Einmal-Passwörter zum Online-Banking könnte einem Einbrecher in die Hände fallen, die gegenüber dem Internet-Verkehr ängstlich gehütete Kreditkartennummer steht auf der arglos weggeworfenen Tankquittung, das Passwort ist leicht erratbar oder an ungesicherter Stelle aufgeschrieben oder der PC wird in eingeschaltetem Zustand verlassen, so dass andere Manipulationen vornehmen können.

4.2 Gefahr an den Endpunkten

Eine Verschlüsselung wirkt nur *zwischen* ihren Endpunkten. Sie sichert die Kommunikation, aber eben nicht die Endpunkte. Ist ein Unberechtigter nicht nur in das Kommunikationsnetz, sondern auch in den Rechner eingedrungen, auf dem die Ver- oder Entschlüsselung vorgenommen wird, so ist der gesamte Verschlüsselungsaufwand vergeblich. Besonders zwei Szenarien spielen hier eine Rolle:

- Liegt ein privater Schlüssel auf einem Rechner, der mit dem Internet verbunden sind, so muss man *immer* mit der Möglichkeit rechnen, dass ein Eindringling auf diesem Rechner Software installiert hat, der den Schlüssel nach außen gibt. Die Tatsache, dass der Schlüssel mit einer "Passphrase" besonders geschützt ist, bedeutet dabei kaum einen zusätzlichen Schutz, wenn etwa ein Tastaturtreiber so verändert wurde, dass die Passphrase mit aufgezeichnet wird. Dass diese Gefahr höchst real ist, wurde durch einen Versuch der Uni Bonn[16] im September 2000 bestätigt, wo es gelang, mehrere Produkte so zu kompromittieren.

- Das oben[17] erläuterte Protokoll "Secure Socket Layer" (SSL) beruht darauf, dass die Verschlüsselung an einem Rechner endet, der über das Internet zugreifbar und damit prinzipiell

[16] `http://www.heise.de/newsticker/data/js-11.06.01-000/`

[17] siehe ☜ 2 auf Seite 6

verwundbar ist. Das ist kein Entwurfsfehler, sondern für automatische Beantwortung von Anfragen aus dem weltweiten Netz unvermeidbar, etwa bei einem WWW-Server mit HTTPS oder einem Zugang zu einem E-Mail-Briefkasten mit IMAP. Kritisch wird die Sache erst, wenn sich ein Benutzer auf diese Sicherheit verlässt. Wenn man also Daten in ein WWW-Formular eingibt, das mittels HTTPS gesichert ist und wenn man dabei auf korrekte Zertifikate (siehe jedoch den nächsten Abschnitt!) achtet, dann kann man einigermassen sicher sein, dass die Daten unverfälscht und vertraulich auf dem Server ankommen, nicht aber, dass sie nach Entschlüsselung dort unverfälscht und vertraulich weitergeleitet werden, und zwar auch dann nicht, wenn die Gefährdung durch den am Zielrechner vorhandenen privaten Schlüssel des Servers vermieden wird.

Für den Versand einer Nachricht, die sicher vertraulich sein soll, ist also SSL *allein* nicht ausreichend; vielmehr braucht man dazu ein Protokoll, bei dem der Empfänger entscheiden kann, wann und wo er die Entschlüsselung vornimmt. Wird dann die Nachricht im noch verschlüsselten Zustand auf einen nicht vom Internet aus zugänglichen Rechner übertragen und erst dort entschlüsselt, so wird diese Schwachstelle vermieden.

Eine deutliche Verbesserung lässt sich bei diesem Problem erzielen, wenn der private Schlüssel nicht auf einem vom Rechner direkt zugreifbaren Speicher liegt, und zwar auch nicht verschlüsselt, sondern auf einer speziellen Karte, die auch gleich die Verschlüsselung mit erledigt. Ein Angreifer, der im schlimmsten Fall wirklich den ganzen Rechner unter Kontrolle bekommt, könnte dann zwar die Karte zum Signieren mitbenutzen, aber wenigstens nicht den privaten Schlüssel mitnehmen und völlig ungestört und unbeobachtbar *woanders* einsetzen. Besonders wenn die Karte nur bei Bedarf eingeschoben wird (das geht bei Serverdiensten natürlich nicht), ist das eine wesentliche Verbesserung der Sicherheit.

4.3 Zertifizierung und Kommerz


5

Die Idee der Zertifizierung von WWW-Servern ist, dass sich der Server durch ein Zertifikat ausweist, das von einer Zertifizierungsstelle (Certification Authority, CA) signiert ist. Der Endbenutzer wird sich dann kundig machen, ob er der CA vertrauen will - eine schwierige Aufgabe, denn es ist überhaupt nicht klar, welche *für den Endbenutzer nachprüfbaren* Kriterien er da anwenden will. Außerdem ist es manchmal schwierig, sich das Wurzelzertifikat der CA zu besorgen.

Der Ausweg besteht darin, dass der Anbieter des WWW-Browsers die Zertifikate einiger bekannter CAs mitliefert. Im angeblichen Interesse, wenn auch nicht im Auftrag des Benutzers hat der Browserhersteller im Verein mit den Zertifizierungsstellen diese schon als besonders vertrauenswürdig eingestuft, in der Regel nach Zahlung eines stolzen Sümmchens durch den Zertifizierer.

Vorsicht Falle: Dabei sind meistens auch Zertifikate von solchen CAs, die *keinerlei* oder nur eine oberflächliche Identitätsprüfung vornehmen, manche davon tragen im Namen "Class 0" bzw. "Class 1". Solange auch nur ein nicht vertrauenswürdiges dabei ist, ist die gesamte Zertifikatsverwaltung im Browser völlig sinnlos, da jeder Unberechtigte sich ja ein Zertifikat einer solchen Institution besorgen kann. Man wird also in den sauren Apfel beißen müssen und in mühsamer Kleinarbeit alle diese Zertifikate entweder löschen oder doch wenigstens in den Zustand versetzen, dass vor ihrer Verwendung eine Anfrage an den Benutzer hochkommt. Es ist nicht herauszubekommen, ob diese Hintertüren für Unberechtigte vorsätzlich oder fahrlässig eingebaut werden; auf jeden Fall hinterlassen sie einen recht faden Geschmack, was die Zuverlässigkeit der betreffenden Zertifizierer im Umgang mit den ihnen anvertrauten Daten angeht.

Aber auch, wenn das nicht der Fall ist, entpuppt sich beim näheren Hinsehen als potenzielle Sicherheitslücke, was ursprünglich als Dienstleistung im Sinne der Benutzersicherheit gedacht war. Dazu muss man sich ansehen, wer welche Interessen hat:

- Der Anbieter des zertifizierten WWW-Angebots hat von der zusätzlichen Sicherheit wenig. Er lässt den Server zertifizieren, damit seine Leser nicht durch für die unverständliche Warnungen, der Unterzeichner eines Zertifikats sei nicht vertrauenswürdig oder unbekannt, vom Lesen abgeschreckt werden.

- Der CA-Betreiber verdient Geld damit, dass WWW-Anbieter ihre Server bei ihm zertifizieren lassen. Das werden sie nur tun, wenn damit die hässliche Warnung für die Benutzer wegfällt, die die Endkunden abschreckt. Deswegen wird der CA-Betreiber den Browser-Anbieter dafür bezahlen, dass seine CA unter den mit dem Browser mitgelieferten CA-Zertifikaten vertreten ist.

- Der Browser-Anbieter schließlich kann an der ganzen Sache nur verdienen, wenn er durchsetzt, dass die Liste der von ihm favorisierten CAs (also die für den Eintrag bezahlt haben) wirklich benutzt wird. Meldungen über nicht verifizierbare Zertifikate werden gerne besonders abschreckend formuliert.

Wenn nun der Endbenutzer auf die Idee kommt, seine eigenen Vorstellungen über die Glaubwürdigkeit von CAs durchzusetzen, lohnt sich das Geschäft nicht mehr für alle Beteiligten. Dagegen muss vorgegangen werden:

- Netscape beispielsweise ernennt bei jedem Versionswechsel alle standardmäßig als vertrauenswürdig eingestuften CAs erneut für vertrauenswürdig, auch wenn ihnen der Benutzer vorher explizit durch Löschung das Vertrauen entzogen hatte. Der Benutzer wird natürlich nicht darauf hingewiesen, dass er nach Netscapes Urteil jemandem erneut zu vertrauen hat.

- Microsoft-Produkte gehen einen Schritt weiter: sie nehmen von Windows XP an dem Endbenutzer die Enscheidung über die Vertrauenswürdigkeit von CAs vollständig aus der Hand. In der Dokumentation[18] heißt das so:

  > New root certificates are no longer available with Microsoft Internet Explorer. Any new roots accepted by Microsoft are available to Windows XP clients through Windows Update. When a user visits a secure Web site (that is, by using HTTPS), reads a secure e-mail (that is, S/MIME), or downloads an ActiveX control that uses a new root certificate, the Windows XP certificate chain verification software checks the appropriate Windows Update location and downloads the necessary root certificate. To the user, the experience is seamless. The user does not see any security dialog boxes or warnings. The download happens automatically, behind the scenes.

  Mit anderen Worten, der Endbenutzer ist *gezwungen*, eine CA als vertrauenswürdig zu betrachten, wenn dies die Firma Microsoft tut. Ein eigenes Urteil steht ihm nicht zu. Wenn man nicht sowohl die Zuverlässigkeit des Urteils von Microsoft wie auch die Unverwundbarkeit ihrer zentralen "Windows Update location" ausgesprochen optimistisch einschätzt, darf man diese Produkte nicht mehr im Zusammenhang mit Anwendungen einsetzen, bei denen Zertifikate überprüft werden müssen.

Dieses Beispiel ist recht ausführlich dargestellt worden, um zu zeigen, wie das Bequemlichkeitsinteresse des Endbenutzers und das kommerzielle Interesse der beteiligten Firmen eine Sicherheitsmaßnahme zur Farce werden lassen können. Im Grunde ist es sogar noch schlimmer: dem Benutzer wird auch noch vorgegaukelt, man kümmere sich um seine Sicherheit. Gerade wenn jemand dubiose Geschäfte machen will, wird er sich seinen Server zertifizieren lassen, um beim Endkunden Vertrauen zu gewinnen. Zertifiziert wird ja schließlich nicht die Seriosität des Geschäfts, sondern lediglich der Zusammenhang zwischen dem Namen des WWW-Anbieters und seinem WWW-Server.

[18] `http://www.microsoft.com/TechNet/itsolutions/security/news/rootcert.asp`

4.4 Elektronische Signaturen sind keine Unterschriften

Trotz ihres Namens haben elektronische Signaturen ganz andere Eigenschaften als herkömmliche eigenhändige Unterschriften:

- Eine eigenhändige Unterschrift kann gefälscht werden, wobei es auf das Geschick des Fälschers ankommt, wie leicht die Fälschung erkannt werden kann. Eine elektronische Signatur kann praktisch nicht gefälscht werden.

- Die Fälschung einer eigenhändigen Unterschrift unterscheidet sich von einer echten, so dass sie oft mit kriminalistischen Mitteln aufgedeckt werden kann. Mit anderen Worten: eine überprüfbar echte Unterschrift kann nur der Unterzeichnende selbst leisten. Demgegenüber kann eine perfekte elektronische Signatur von jedem angebracht werden, der im Besitz des privaten Schlüssels ist. Auch wenn das ein Unberechtigter sein sollte, unterscheidet sich die Signatur in keiner Weise von einer echten.

Das Gegenstück zur elektronischen Signatur ist daher nicht die eigenhändige Unterschrift, sondern so etwas wie ein unfälschbares perfektes Siegel: man braucht es zur Unterzeichnung unbedingt, aber wer es hat, kann damit beliebig viele Dokumente unterzeichnen.

Noch in einer zweiten Eigenschaft unterscheiden sich elektronische Signaturen von herkömmlichen eigenhändigen Unterschriften. Wer seinen Namen mit der Hand unter ein Schriftstück setzt, sieht mit eigenem Auge, was er unterschreibt; wer dagegen an einem Dokument eine elektronische Signatur anbringt, ist darauf angewiesen, dass die Software ihm genau den Text anzeigt, der dann auch signiert wird. Wenn sich elektronische Signaturen durchgesetzt haben, werden aber die meisten Nutzer nicht das Wissen haben, das überprüfen zu können.

4.5 Also Vorsicht!

Wenn beim Einsatz von Verschlüsselungstechniken so viele Gefahren lauern, sollte man es da nicht lieber bleiben lassen? In der folgenden Zusammenfassung wird darauf eine Antwort versucht:

- Geht es nur um die Sicherung der Kommunikation, also nicht etwa um die Erstellung dauerhafter signierter Urkunden, so wird man nichts falsch machen, wenn man sich zum Einsatz sichererer Techniken entschließt. Beispielsweise ist verschlüsselte Kommunikation immer sicherer als unverschlüsselte, selbst wenn der Kommunikationspartner nicht authentisiert wird. Man muss nicht immer alle Geschütze gleichzeitig auffahren.

- Der voranstehende Punkt gilt nicht, wenn man sich dazu verleiten lässt, wegen *einer* Sicherheitsmaßnahme andere für überflüssig zu halten. Jede zusätzliche Maßnahme erhöht zwar die Sicherheit, aber jede deckt nur bestimmte Risiken ab und lässt andere Risiken bestehen; darüber muss man sich immer Rechenschaft ablegen.

- Werden Dokumente digital signiert, können zusätzliche Sicherungen auch zusätzliche Risiken bergen, nämlich dann, wenn der private Schlüssel in unbefugte Hände gerät. Dann können Unberechtigte nämlich nicht nur die Kommunikation belauschen (was sie im ungesicherten Fall ohnehin gekonnt hätten), sondern glaubhaft in fremdem Namen handeln.

- Ein Rechner, der ans Internet angeschlossen ist, ist prinzipiell gefährdet, belauscht zu werden und zwar auch während der Zeiten, in denen er vorübergehend vom Netz getrennt ist. Ein solcher Rechner sollte daher nicht für solche Aufgaben benutzt werden, bei denen ein Einbruch unabsehbare Folgen haben kann, wie

- zum Signieren von Dokumenten, die nicht nur während einer kurzen Zeitspanne Bedeutung haben,
- zum Signieren von Zertifikaten, außer wenn der unberechtigte Einsatz der so beglaubigten Zertifikate klar unkritisch ist, etwa nur zu Testzwecken oder nur zum Zugang in schwach gesicherte Netze,
- zum Signieren von Zertifikaten, die den Schlüssel von anderen Zertifizierungsstellen beglaubigen,
- zum Signieren, zum Verschlüsseln oder zum Entschlüsseln von Dokumenten, die sicher geheim bleiben sollen.

5 Rechtliches

Über die rechtliche Relevanz digitaler Signaturen herrschen unter juristischen Laien sehr verschiedene Vorstellungen. Da der Verfasser dieses Artikels selbst juristischer Laie ist, darf man von diesem Abschnitt keinesfalls eine endgültige Klärung der offenen Fragen erwarten. Der Blick vom naiven Laienstandpunkt könnte aber die Grundlinien klarer hervortreten lassen als das in einem juristischen Fachartikel, der dann auch alle Grenzfälle mit betrachten muss, möglich wäre.

Im Jahre 2001 sind in Deutschland eine Reihe von Gesetzesänderungen über elektronische Signaturen in Kraft getreten. Es ist aber nun nicht so, dass erst durch diese Gesetze die Anbringung elektronischer Signaturen rechtliche Folgen haben kann oder dass jetzt solche Folgen nur dort eintreten können, wo diese Gesetze greifen:

- Neu ist nur die Möglichkeit, *Urkunden* mit elektronischen Signaturen zu erstellen. Geregelt ist das durch zwei Gesetze, nämlich
  - das Signaturgesetz (SigG)[19], welches definiert, unter welchen Bedingungen eine "qualifizierte" elektronische Signatur zustandekommt, der dann in *anderen* Gesetzen eine besondere rechtliche Relevanz zugesprochen werden kann und
  - das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr[20], mit dem solche Gesetze geändert wurden, in denen festgelegt wird, mit welchen Mitteln Urkunden erstellt werden, also insbesondere das Bürgerliche Gesetzbuch (BGB) und die Zivilprozessordnung (ZPO), aber auch viele andere.

  Völlig unabhängig von all diesen Regelungen steht es jedem Richter frei, eine elektronische Signatur, sei sie nun qualifiziert oder nicht, bei der Beweiswürdigung in einem Prozess für glaubwürdig zu halten und einem so signierten Dokument mehr zu vertrauen als einem unsignierten, auch wenn es keine Urkunde im Sinne der beiden eben genannten Gesetze ist. Schließlich werden auch sonst in Prozessen alle möglichen Beweismittel vorgelegt, die keine Urkunden sind.

Der Grenzbereich zwischen diesen beiden Punkten, also die Frage, inwieweit eine elektronisch signierte Urkunde ein "besseres" Beweismittel ist als ein anderes und wer im Zweifel die Beweislast dafür trägt, dass alle Signaturen gesetzeskonform zustandegekommen sind, ist eine Frage für die Diskussion unter Juristen[21] und gehört deswegen nicht hierher.

[19] `http://www.netlaw.de/gesetze/sigg.htm`
[20] `http://www.kanzlei.de/afpmrg.htm`
[21] `http://ruessmann.jura.uni-sb.de/rw20/people/ruessmann/Elbeweis/elbeweis.htm`

Wie weiter oben[22] erläutert, haben elektronische Signaturen ganz andere Eigenschaften als herkömmliche Unterschriften. Welche Folgen das im Rechtsverkehr hat, kann nicht durch Gesetze festgelegt werden, sondern wird sich erst in den kommenden Jahren aus der Rechtsprechung ergeben. Eine gewisse Vorsicht im Umgang diesen neuen Möglichkeiten ist also sicher angebracht.

[22] siehe ☜ 6 auf Seite 15