Die digitale Unterschrift

Arno Distel
MT 99, 29198

04.08.2003

Ergänzungslehrgebiet „IT-Sicherheit und Datenschutz“
Dipl.-Wirtsch.-Inf. Jana False, SS 2003
TU Ilmenau

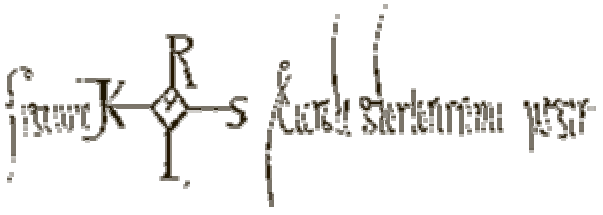
Zusammenfassung

Die Papierform von Dokumenten und Briefen wird immer stärker von der digitalen Kommunikation abgelöst, obwohl sie einen entscheidenden Vorteil hat: Die Rechtsverbindlichkeit und Rechtsgültigkeit kann durch eine einfache handschriftliche Unterschrift gewährleistet werden. Die digitale Unterschrift soll dies als Äquivalent in der Welt der digitalen Kommunikation leisten. Die vorliegende Arbeit zeigt Kriterien für die Akzeptanz und Verbreitung der digitalen Unterschrift auf. Signaturalgorithmen, wie RSA und DSA, sowie die am häufigsten verwendeten Hashfunktionen der MD4-Familie werden vorgestellt. Angriffsmöglichkeiten auf Signatursysteme werden systematisiert und der rechtliche Rahmen zu digitalen Signaturen erläutert.

1 Einleitung

Den Wunsch Willenserklärungen verbindlich abzugeben gibt es schon seit langer Zeit. Erste siegelartige Objekte wurden bereits im Jahre 1.200 vor Christus gefunden. Die Römer brachten ein umfangreiches Justizwesen mit formellen Verträgen hervor. Hierbei war die Authentizität eines Schriftstückes von besonderem Interesse, wofür Siegel und Stempel zum Einsatz kamen. Mit der Ausbreitung des Schrifttums und einem Bewusstsein für Individualität trat später die eigene, persönliche Unterschrift an die Stelle von Siegeln. [www_1]

Ein Beispiel für die lange Tradition der Verwendung von Handzeichen zur Sicherstellung der Authentizität ist die Unterschrift Karls des Großen. Der Kaiser konnte weder Lesen noch Schreiben und unterzeichnete dennoch seine Dokumente mit einem bestimmten Karo zwischen den Buchstaben des Monogramms. Die komplette Unterschrift wurde von einem Schreiber angefertigt. [Glad_95, S.80 f.]



Das neue System „Handzeichen“ musste jedoch erst Vertrauen gewinnen, um den Siegel in weiten Teilen ablösen zu können. Eine hinreichende Sicherheit in der Anwendung und im System an sich musste gewährleistet sein.

Heute, ein paar hundert Jahre später, stehen wir praktisch vor der gleichen Situation: Im globalen Geschäftsverkehr hat die digitale Zustellung von Dokumenten die postalische Zustellung weitestgehend abgelöst. Der herkömmliche Versand dauert vergleichsweise zu lange und ist zu teuer. Die Echtheitsüberprüfung von Unterschriften ist bei häufig wechselnden Vertragspartnern und internationalen Vertragsabschlüssen zudem nur sehr schwer möglich. Hier kommt der Wunsch auf, auch trotz Verwendung von digitalen Medien bei globaler Kommunikation die Authentizität von Willenserklärungen gewährleisten zu können.

Ein digitales Abbild der Unterschrift, als Bit-Map ließe sich zu einfach kopieren und in ein beliebiges anderes elektronisches Dokument an beliebiger Stelle einfügen. Es ist für eine digitale Signatur also anders vorzugehen, um das Vertrauen in das System und in die Anwendung für sich zu gewinnen und um somit die herkömmliche Unterschrift im digitalen Umfeld ersetzten zu können.

Welche Kriterien für eine Akzeptanz von (digitalen) Signaturen zu erfüllen sind, ist Thema des folgenden Kapitels (2). Auf die technische Funktionsweise der bisher vorhandenen Systeme für digitale Signaturen soll im dritten Kapitel eingegangen werden. Sicherheitsbetrachtungen (Kapitel 4) und die sich im Bereich der digitalen Signaturen ergebenden rechtliche Aspekte (Kapitel 5) sollen schließlich in diese Arbeit Einzug finden.

2 Akzeptanz von digitalen Unterschriften

2.1 Funktionen der eigenhändigen Unterschrift

Zunächst stellt sich die Frage, welche Funktionen die herkömmliche eigenhändige Unterschrift erfüllt. Neben der bloßen Authentizität (Echtheitsfunktion) sind dies hauptsächlich folgende [Hrst_96, S.3]:

- Abschlussfunktion — Die eigenhändige Unterschrift bringt den Abschluss oder die Vollendung der Willenserklärung als Ganzes zum Ausdruck. Die Verbindlichkeit wird dadurch festgelegt und das unterschriebene Dokument hebt sich somit vom bloßen Entwurf ab.
- Identitätsfunktion — Die Identität des Ausstellers wird kenntlich gemacht.
- Warnfunktion — Die eigenhändige Unterschrift bietet gewissen Schutz vor Übereilung. Durch den Vorgang des Unterzeichnens soll die rechtliche Bedeutung des Dokuments verdeutlicht werden.

- Beweisfunktion — In einem späteren Streitfall kann die Beweisführung erleichtert werden. Ein unterschriebenes Dokument wird als richtig und vollständig angesehen und ist somit rechtsrelevant.

Die Handunterschrift kann also diese Funktionen für ein Papierdokument bieten und ist ohne großen Aufwand jederzeit und überall verfügbar.

2.2 Anforderungen an digitale Unterschriften

2.2.1 Gewährleistung der herkömmlichen Funktionen

Digitale Signaturen müssen diese Funktionen äquivalent leisten, um die digitale Kommunikation auf mindestens die gleiche Sicherheitsebene zu stellen. Zunächst müssen sie sich ähnlich wie bei der herkömmlichen Unterschrift vom Dokument abheben und sowohl vom Unterzeichner als auch vom Dokument abhängig sein. Durch die digitalen Kopierfunktionen wäre es sonst einfach, die Signatur einem anderen Text zuzuordnen.

Die Gewährleistung der Identitätssicherung des Unterzeichners ist im digitalen Umfeld schwieriger und mit höherem technischem Aufwand realisierbar. Die Echtheit eines Papierdokuments lässt sich häufig schon durch menschliche Intuition erkennen, während auf der digitalen Seite das Vertrauen in Hard- und Software die Basis bilden muss, um die Echtheit der Signatur und somit des Dokuments zu garantieren.

2.2.2 Lösen der durch Übertragung von Dokumenten entstehenden Probleme

Durch die Übertragung von Dokumenten kommen noch weitere Problemfelder hinzu, für die hauptsächlich fünf Schutzziele formuliert werden können, welche die Anforderungen an eine sichere digitale Kommunikation ausdrücken [Bert_01 S.3]:

- Vertraulichkeit — Die Inhalte von Nachrichten sollen gegenüber allen Instanzen, außer dem vorgesehenen Empfänger vertraulich bleiben.
- Integrität — Manipulationen an Nachrichteninhalten sollen erkannt werden können.
- Authentizität — Fälschungen von Absenderangaben sollen erkannt werden können.
- Verfügbarkeit — Das Kommunikationssystem soll den gewünschten Nachrichtenaustausch zwischen Absender und Empfänger ermöglichen.
- Zurechenbarkeit — Das Absenden bzw. Empfangen einer Nachricht soll gegenüber Dritten nachgewiesen werden können.

2.2.3 Verdeckte Informationen in Dokumenten

Ähnlich wie das „Kleingedruckte“ bei herkömmlichen Verträgen ist es bei der Anfertigung von digitalen Dokumenten möglich, weitere Vertragsgegenstände in das

Dokument einfließen zu lassen. Während das „Kleingedruckte“ noch vom Auge lesbar ist und daher eindeutig mitunterschrieben wird, können auf digitaler Seite Informationen derart in das Dokument eingebaut werden, dass es nur von der Darstellungsweise und der Arbeitsumgebung abhängt, ob die Informationen überhaupt wahrgenommen werden können. Eine digitale Signatur muss also sicherstellen, dass sie nur für solche Inhalte gilt, die auch gesehen werden und damit die Informationen zur Darstellung und Arbeitsumgebung beinhalten. [Hrst_96 S.9]

3 Funktionsweise von digitalen Signaturen

3.1 Allgemeine Verwendung von digitalen Signaturen

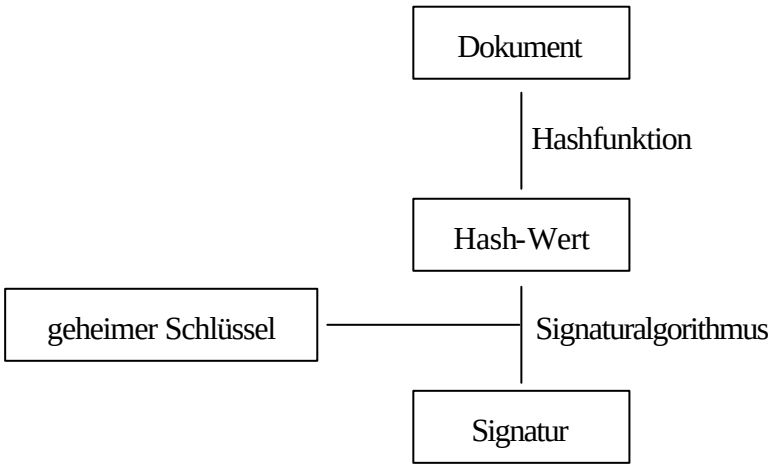
Zunächst erzeugt der Absender eine digitale Signatur *SIG* mit Hilfe eines Signatur-Algorithmus *S* unter Verwendung eines privaten Signierschlüssels. Dabei wird der Signatur-Algorithmus entweder direkt auf die Nachricht *y* angewendet:

$$SIG(y)=S_x(y)$$ [Glad_95 S.97]

oder auf den aus *y* erzeugten Hash-Wert *H(y)* angewendet:

$$SIG(y)=y||S_x(H(y))$$ [Glad_95 S.98]

Die Erzeugung eines Hash-Wertes (als Prüfsumme) ist als Einwegfunktion zu bezeichnen. Aus dem Hash-Wert kann das Dokument praktisch nicht rekonstruiert werden.



Die Signatur wird an die zu übermittelnde Nachricht angehängt, verschlüsselt also die eigentliche Nachricht nicht vor den Augen unbestimmter Empfänger.
Zur Überprüfung der Echtheit eines Dokumentes benutzt der Empfänger einen gesonderten Algorithmus, wobei hier ein öffentlicher Schlüssel verwendet wird. Der Vorteil der Verwendung eines Hash-Wertes als Grundlage der Signatur liegt darin, dass sowohl das Signieren als auch die Echtheitsprüfung der Signatur schneller geschieht.

Das Verfahren der digitalen Signatur basiert also auf asymmetrischen Verschlüsselungssystemen mit Schlüsselpaaren: Der Absender verschlüsselt mit einem privaten Schlüssel, der Empfänger kann mit einem öffentlichen Schlüssel, die Echtheit des Dokumentes prüfen.

Durch die Verwendung von Signaturen kann die Modifikation von Daten zwar nicht verhindert werden, allerdings stimmt bei geänderten Daten die Prüfsumme des Empfängers nicht mehr mit der Prüfsumme des Absenders überein und die Nachricht kann verworfen bzw. eine neue Übertragung vorgenommen werden.

3.2 Signaturalgorithmen

Für die Praxis werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zurzeit folgende Signaturalgorithmen empfohlen. [www_2] und [www_3]

3.2.1 RSA

Das nach seinen Erfindern Rivest, Shamir und Adleman benannte RSA-Verfahren wurde im Jahr 1977 entwickelt. Das Verfahren beruht auf Primzahlenfaktorisierung und gilt als sicher, wenn der so genannte Modulus $n=pq$ (p und q Primzahlen) eine Bitlänge von 1024 hat. Ab dem Jahr 2006 empfiehlt das BSI die Erhöhung auf 2048bit, wobei die Sicherheit dann bis Ende 2007 gewährleistet wird. Die beiden Primfaktoren p und q sollten die gleiche Größenordnung haben, aber nicht zu dicht beieinander liegen. Es wird eine weitere Zahl e als so genannten öffentlichen Exponenten gesucht, die kleiner als der Modulus n ist und folgende Bedingung erfüllt ist:

$$ggT(e,(p-1)(q-1))=1$$

Als weitere Zahl d, den geheimen Exponenten wird berechnet:

$$e*d=1 \bmod kgV(p-1,q-1)$$

Der öffentliche Schlüssel besteht dann aus dem Paar (n, e), der geheime Schlüssel ergibt sich aus (n, d). Die beiden Primfaktoren p und q können nach der Berechnung der Schlüssel gelöscht werden oder müssen mit dem geheimen Schlüssel aufbewahrt werden. Die Sicherheit basiert darauf, dass es derzeit schwer ist, den geheimen Schlüssel aus dem öffentlichen Schlüssel zu generieren. Würde es gelingen n in p und q zu faktorisieren, dann wäre der geheime Exponent d zu finden, was aber derzeit durch die besten Faktorisierungsalgorithmen (noch) nicht möglich ist.

Soll eine Nachricht m_1 von Alice an Bob (die am meisten verwendeten Personen, wenn es um Signaturen und Verschlüsselungen geht) gesendet werden, würde die Signatur folgendermaßen ablaufen:

- Alice generiert die digitale Signatur $s=m_1^d \bmod n$ (n und d sind privater Schlüssel)
- Sie sendet m_1 und s an Bob

- Er schaut, ob $m_2=s^e \bmod n$ identisch mit der übertragenen Nachricht m_1 ist (n und e sind öffentlicher Schlüssel)

3.2.2 DSA (Digital Signature Algorithm)

Ähnlich wie das Faktorierungsproblem bei RSA basiert der DSA ebenfalls auf einem mathematischen Problem: Das diskrete Logarithmusproblem. [Petr_96 S.10]
Es sind zunächst zwei Elemente *g* und *h* einer Gruppe *G* gegeben: Es wird eine Zahl gesucht, so dass gilt:

$$g^x = h$$

Werden beispielsweise folgende Werte betrachtet:

$$3^x = 13 \bmod 17$$

wäre die Lösung *4*, da

$$3^4 = 81 = 13 \bmod 17$$

Als Elemente der Gruppe G werden ebenfalls Primzahlen verwendet. Unterschiede bestehen in der Berechnung des Signierens und der Signaturüberprüfung. Während beim RSA-Verfahren die Überprüfung schneller berechnet werden kann, als das Generieren von Signaturen ist es beim DSA umgekehrt. Da jedoch oft ein Dokument einmalig signiert wird und die Verifikation häufiger durchgeführt wird, ist das als Nachteil des DSA aufzufassen.
Der DSA wird im DSS (Digital Signature Standard) verwendet, welcher vom National Institute of Standards and Technology (NIST) und der National Security Agency (NSA) zum Signaturstandard der US-Regierung erklärt wurde. Auch das BSI hält den DSA für sicher, wenn der Parameter *x* eine Länge von mindestens 1024 bit besitzt.

3.3 Hashfunktionen

Im Bereich der verschiedenen Hashfunktionen spielt die MD4 Familie eine Hauptrolle. Die derzeit weltweit am meisten implementierte Funktion ist MD5. Vom BSI wird hauptsächlich SH1 und RIPEMD-160 für die Anwendung in den nächsten Jahren bis 2007 empfohlen. [Hrst_96 S. 84] [www_2] [www_3]

3.3.1 MD4, MD5 (Message Digest)

Diese beiden Hashfunktionen bilden aus einem Text mit beliebiger Länge einen 128 bit Hash-wert. Die 1990 von Rivest entwickelte Version MD4 hängt zunächst an den Text einen Anhang an, so dass die Länge des Textes plus 64 bit durch 512 teilbar ist. Eine 64 bit große Entsprechung des Textes wird dann angehängt und der gesamte Text in 512 bit großen Blöcken verarbeitet, wobei jeder Block in 3 Durchläufen komprimiert wird. Nachdem Attacken teilweise zu Kollisionen für MD4 führten, wurde ein Jahr später die Version MD5 entwickelt. Die Kompression wird hier in 4 Durchläufen durchgeführt. Zu den genanten Versionen kann noch Extended MD4 genannt werden, was eine verstärkte

Variante von MD4 ist: Der Hash-Wert hat eine Länge von 256 bit; die Kompressionsfunktion besteht aus zwei parallelgeschalteten Strängen der MD4-Kompressionsfunktion, hat also 6 Durchläufe.
MD5 wird von Rivest´s Firma hauptsächlich empfohlen, für extrem-kritische Anwendungen lautet die Empfehlung zu Extended MD4. Die Anwendung von MD4 ist um circa 30% schneller als von MD5, weshalb für Anwendungen, bei denen die Performance den Vorrang hat, auch MD4 bei eingeschränkter Sicherheit noch verwendet werden kann.

3.3.2 SHA-1 (Secure Hash Algorithm)

Der SHA gehört zur MD4 Familie und wurde von NSA und NIST veröffentlicht. Die Länge des Hash-Wertes beträgt hier 160 bit. Die Kompressionsfunktion besteht aus 4 Runden, wobei im Gegensatz zu den unter 3.3.1 genannten MD4 Funktionen eine Runde aus 20 statt 16 Schritten besteht. Der Algorithmus ist langsamer als MD5, bietet allerdings eine höhere Sicherheit durch den längeren Hash-Wert.

3.3.3 RIPEMD-160

Diese Funktion liefert ebenfalls einen 160 bit langen Hash-Wert. Die Kompressions-funktion besteht aus zwei parallelgeschalteteten Strängen mit je 5, also insgesamt 10 Runden. Damit ist dieser Algorithmus der langsamste der genannten.

3.3.4 Tiger

Die Entwicklung von sicheren Hashfunktionen ist als nicht schwer anzusehen. Das Hauptproblem liegt in der Performance, also sichere Funktionen, die zugleich auch schnell sind zu konstruieren. Ein Versuch ist die Hashfunktion Tiger, die im Gegensatz zu den bisher genannten statt für 32 bit Prozessoren speziell für 64 bit Prozessoren entwickelt wurde. Tiger kann Hash-Werte von 128, 160 und 192 bit Länger erzeugen und ist dabei gegenüber MD5 fast 3,5-fach schneller.

3.4 Personenidentifikation durch digitale Signaturen

Die bisher beschriebenen Signaturalgorithmen in Kombination mit den aufgezeigten Hashfunktionen zeigen eine Manipulation an den digital signierten Daten sehr gut an. Soll jedoch mit der digitalen Signatur auch die Identifikation der Person gewährleistet werden, die die Signatur geleistet hat sind weitere Maßnahmen erforderlich. Da jeder behaupten kann, der zur Verfügung gestellte öffentliche Schlüssel gehöre zu einer bestimmten Person, ist es für den Empfänger bei der Überprüfung der Signatur nicht möglich, Rückschlüsse auf die wirkliche Person zu ziehen.

Hierfür ist eine unabhängige Instanz nötig, der beide Parteien vertrauen und die bestimmte öffentliche Schlüssel bestimmten realen Personen zuweisen. Diese Instanzen – Zertifizierungsstellen genannt – stellen für einen öffentlichen Schlüssel ein Zertifikat aus, nachdem sich der Inhaber des Schlüssels gegenüber der Zertifizierungsstelle identifiziert

hat. Die Identifikation kann im einfachsten Fall über E-Mail erfolgen, wobei dies eine eher geringe Aussage über die Identität des E-Mail Absenders ist. Daher ist es üblich, die Identifikation über die Vorlage eines Personalausweises oder Reisepasses vorzunehmen. Das ausgestellte Zertifikat wird dem Inhaber des Schlüssels überreicht, ist aber auch im Internet in einem Verzeichnis der Zertifizierungsstelle einzusehen und somit für jeden Empfänger zu überprüfen.

3.5 Zeitfunktionen von digitalen Signaturen

Die Zertifizierungsstellen stellen die Zertifikate nur für einen vorab bestimmten Zeitraum aus. Die Länge des Gültigkeitszeitraums wird durch Faktoren, wie Vertragsdauer mit dem Teilnehmer und technischen Anforderungen wie Wahl der kryptographischen Parameter bestimmt. Auch vor Ablauf des Gültigkeitszeitraums ist eine Sperrung des Zertifikats sowohl von der Zertifizierungsstelle als auch vom Inhaber des Zertifikats möglich. Sollte das kryptographische Verfahren nicht mehr geeignet sein oder der Signaturschlüssel des Inhabers kompromittiert sein ist dies für die Sicherheit der digitalen Signatur notwendig. Hier ist also der Zeitpunkt des Signierens wichtig. Nur wenn das dabei verwendete Zertifikat zu dem Zeitpunkt Gültigkeit besitzt ist die Signatur gültig und somit ist eine Zeitangabe in der eigentlichen Signatur notwendig.

Es kommen hierbei verschiedene Methoden zum Einsatz: Im einfachsten Fall macht der Unterzeichner selbst Angaben über den Zeitpunkt des Signierens. Manipulationssicherheit der Uhrzeit kann durch Zeitstempeldienste, eine vertrauenswürdige Instanz, die eine digitale Bescheinigung liefert, dass ihr bestimmte Daten (als Hash-Wert) zu einem bestimmten Zeitpunkt vorgelegen haben, erreicht werden. Alternativ können auch Zeitstempelboxen verwendet werden, die meist mit einem Funkempfänger für das DCF-77 Zeitsignal ausgestattet sind und lokal beim Unterzeichner zum Einsatz kommen. Dies bietet den Vorteil, dass keine externe Kommunikation stattfindet und somit keine Benutzerprofile oder ähnliches über den Signierer erstellt werden können. [Bert_01 S.158 ff.]

4 Sicherheitsbetrachtungen zu digitalen Signaturen

4.1 Angriffsstufen

Der Zentrale Aspekt bei der Betrachtung der Sicherheit der Signaturverfahren ist, in wie weit sich der geheime Schlüssel brechen lässt. Hier lassen sich mehrere Stufen des Angriffs unterscheiden. [Bert_01 S.12] [Petr_96 S.24 f.]

4.1.1 Vollständiges Brechen

Die sicherlich höchste Stufe ist das vollständige Brechen der Signatur. Hier wird der geheime Schlüssel gefunden und der Angreifer hat somit die Möglichkeit selbst digitale

Signaturen herzustellen, die von denen des echten Signierers nicht unterscheidbar sind. Wurde mit dem Schlüssel auch der eigentliche Nachrichtentext verschlüsselt, so kann zu allen mit diesem Schlüssel verschlüsselten Nachrichten der Klartext ermittelt werden.

4.1.2 Universelles Brechen – Globale Deduktion

Durch einen äquivalenten Algorithmus ist es dem Angreifer ebenso möglich, identische Signaturen für beliebige Nachrichten zu erzeugen. Er besitzt die gleichen Möglichkeiten wie der Inhaber des Schlüssels, hat aber keine Kenntnis über den geheimen Schlüssel erhalten. Ebenso wie beim vollständigen Brechen können auch alle damit verschlüsselten Nachrichten in den Klartext überführt werden.

4.1.3 Nachrichtenbezogenes Brechen – Lokale Deduktion

Der Angreifer findet für einzelne Nachrichten ohne Kenntnis des geheimen Schlüssels eine gültige digitale Signatur. Je nach Ursprung des Textes wird unterschieden zwischen
a) selektivem Brechen, wenn der Angreifer die Nachricht selbst wählt und
b) existentiellem Brechen, wenn es sich um eine Nachricht handelt, die der Angreifer jedoch nicht selbst gewählt hat.

4.1.4 Informationsdeduktion

Der geheime Schlüssel wird dem Angreifer bekannt, ohne dass das Kryptosystem selbst gebrochen wird. Dies kann durch Zugriff auf den Schlüssel durch Schwachstellen in Anwendungsprogrammen oder auch durch die bloße Weitergabe der Information geschehen.

4.2 Angriffsarten

In Abhängigkeit der Informationen, die einem Angreifer zur Verfügung stehen, können folgenden Angriffsarten unterschieden werden. [Petr_96 S.24]

4.2.1 Direkter Angriff

Der Angreifer nutzt nur die Kenntnis des Signaturverfahrens, der Systemparameter und des öffentlichen Schlüssels des Signiereres aus.

4.2.2 Angriff mit bekannter Signatur

Dem Angreifer ist zu einer von ihm nicht gewählten Menge von Dokumenten die Signatur bekannt.

4.2.3 Ungerichteter Angriff

Der Angreifer wählt einmalig eine Menge von Dokumenten aus und lässt sie vom Signierer unterzeichnen.

4.2.4 Gerichteter Angriff

Der Angreifer erzeugt einmalig spezielle Dokumente unter Berücksichtigung des öffentlichen Schlüssels sowie bereits bekannter Signaturen und lässt sie unterzeichnen.

4.2.5 Adaptiver Angriff

Der Angreifer legt dem Signierer wiederholt speziell ausgewählte Dokumente, wie beim gerichteten Angriff zur Unterzeichnung vor.

4.3 Zusammenfassung der Angriffe

Für die Sicherheit eines Systems ist der jeweils schwächste Angriff mit dem eine Brechungsstufe erreicht wird maßgebend. Nicht akzeptabel sind Systeme, die erfolgreiche Angriffe nach 4.1.1 bis 4.1.3a ermöglichen. Ein existentielles Brechen kann ohne Folgen bleiben, wenn die brechbaren Nachrichten keine sinnvollen Nachrichten sind und im Verhältnis zu der Menge aller möglichen Nachrichten sehr klein sind. Ein solches System wird aber meist dennoch nicht als akzeptabel angesehen. Da ein Angriff nach 4.1.4 kein eigentliches Brechen des Kryptosystems ist, ist dies kein Beweis dafür, dass das System inakzeptabel ist. Höchstens die technische und organisatorische Umsetzung kann als unzureichend beschrieben werden.

Als besonders sicher gilt ein Verfahren, wenn es unter der stärksten Angriffsart, also dem adaptiven Angriff nach 4.2.5 nicht existentiell nach 4.1.3b zu brechen ist. In der Praxis sind solche Verfahren allerdings nicht bekannt. Das existentielle Fälschen kann durch die Verwendung von Hashfunktionen vermieden werden, so dass ein Signaturverfahren als sicher gilt, wenn es unter einem adaptiven Angriff nicht universell zu brechen ist.

5 Rechtliche Aspekte

Um rechtswirksame Willenserklärungen mit Hilfe der digitalen Signatur abzugeben reicht jedoch die technische Konzeption eines Signaturalgorithmus nicht aus. Nur gesetzliche Rahmenbedingungen können Sicherheit in der rechtlichen Interpretation von digital signierten Dokumenten liefern.

5.1 Europäische Richtlinie zu elektronischen Signaturen

Auf europäischer Basis ist die Notwendigkeit einer gesetzlichen Rahmenbedingung erkannt worden und wird durch die europäische Richtlinie zu elektronischen Signaturen repräsentiert.

5.2 Signaturgesetz SigG, Signaturverordnung SigV

Das SigG bildet die technische Umsetzung der EU-Richtlinien in Deutschland. [www_4] Das Gesetz ist in sechs Abschnitte unterteilt. Geregelt sind in diesen Abschnitten folgende Schwerpunkte:

1.Abschnitt Zweck, Anwendungsbereich des SigG, Zuständige Behörde und Begriffsbestimmungen

2.Abschnitt	Zertifizierungsdienstanbieter
3.Abschnitt	Freiwillige Akkreditierung der Zertifizierungsdienstanbieter
4.Abschnitt	Technische Sicherheit
5.Abschnitt	Aufsicht
5.Abschnitt	Bußgeldvorschriften, Ausländische elektronische Signaturen, Rechtsverordnung, Übergangsvorschriften

Die Signaturverordnung regelt die genaue Arbeitsweise der Zertifizierungsdiensteanbieter.

5.3 Rechtsgültigkeit von digitalen Signaturen

Da das SigG und die SigV nur die technische Umsetzung und Ausgestaltung der digitalen Signaturen als Inhalt haben sind weitere gesetzliche Regelungen notwendig, um der digitalen Signatur eine mindestens gleich hohe Rechtsgültigkeit und Rechtsverbindlichkeit wie der herkömmlichen handschriftlichen Unterschrift zu gewährleisten. Dies regelt im privatrechtlichen Bereich das Formanpassungsgesetz und im öffentlichen Recht ein noch zu erarbeitendes Gesetz. Weiterhin müssen eine Reihe von Spezialgesetzten überprüft und angepasst werden. Der Status einer eindeutigen gesetzlichen Regelung ist aber derzeit noch nicht erreicht. [www_5]

6 Ausblick

Zusammenfassend lässt sich feststellen, dass die digitale Signatur die herkömmliche Unterschrift bei weitem noch nicht abgelöst hat und auch als passende Ergänzung noch keinen hohen Stellenwert erlangt hat. Dies ist weniger in den technischen Aspekten zu sehen. Die Sicherheit ist hier in vielerlei Hinsicht der handschriftlichen Unterzeichnung ebenbürtig oder bietet eine höhere Sicherheit. Hauptursache für die eher schleichende Verbreitung von digitalen Signaturen ist im rechtlichen Bereich zu sehen. Hier sind, gerade auf internationaler Ebene hinreichende Regelungen noch nicht getroffen worden.

Allgemein lässt sich die Tendenz beobachten, dass die Industrie auf Signale der Politik wartet, um praktisch ausgereifte Methoden für digitale Signaturen auf den Markt zu bringen, während die Politik sich nicht dafür zuständig sieht genaue Vorgaben für eventuelle Geschäftsmodelle zu geben. [www_6]

Eine eventuelle Lösung des Problems bietet das am 3.April 2003 gegründete „Bündnis für elektronische Signaturen“, welches seine Ziele bis Ende 2005 umgesetzt haben will [www_7]. Doch auch hier ist anzunehmen, dass der Hauptfaktor für eine breite Akzeptanz und Nutzung von elektronischen Signaturen darin liegt, dass vor allem die Einheitlichkeit gewährleistet sein muss. Erst wenn die digitale Signatur so einfach und einheitlich anzuwenden ist, wie eine Unterschrift mit einem Kugelschreiber auf einem Papierdokument wird sie sich im Alltag etablieren.

Literatur

[Bert_01] Bertsch, Andreas: *Digitale Signaturen*. Springer, Berlin u.a., 2001, 264 S.

[Glad_95] Glade, Albert, ... (Hrsg.): *Digitale Signatur & Sicherheitssensitive Anwendungen*. Vieweg, Braunschweig u.a., 1995; 279 S.

[Hrst_96] Horster, Patrick (Hrsg.): *Digitale Signaturen. Grundlagen, Realisierungen, Rechtliche Aspekte, Anwendungen*. Vieweg, Braunschweig u.a., 1996, 248 S.

[Petr_96] Petersen, Holger: *Digitale Signaturverfahren auf der Basis des diskreten Logarithmusproblems und ihre Anwendungen*. Shaker, Aachen, 1996, 277 S.

[www_1] http://ig.cs.tu-berlin.de/ap/rg/1998-04/geschichte.html

[www_2] http://www.bsi.bund.de/esig/index.htm

[www_3] http://www.rsasecurity.com/rsalabs/faq/3.html

[www_4] http://www.bundesregierung.de/Gesetze/-,7214/Gesetze-A-Z.htm

[www_5] http://www.bsi.de/esig/faq/lawnordr.htm

[www_6] http://www.heise.de/ct/02/13/047/default.shtml

[www_7] http://www.heise.de/newsticker/data/ad-03.04.03-000/