Hon. Prof. Dipl.-Ing. Dr. Kurt Judmann

Elektronische Signaturen und ihre Anwendung

1. Einleitung

Dokumente werden im geschäftlichen Bereich zum weitaus überwiegenden Teil mit Hilfe von Computersystemen und entsprechenden Programmen erstellt. Durch die weitgehende Anbindung der Computer an das Internet, ergibt sich die Nutzung der dadurch verfügbaren Kommunikationsmethoden zur elektronischen Übertragung von Dokumenten. Im einfachsten Fall handelt es sich dabei um die Übermittlung von Nachrichten, bei denen es primär auf die rasche Informationsübermittlung ankommt, in Form von E-mails. Sehr weit verbreitet ist darüber hinaus auch die Übermittlung von elektronischen Versionen von Schriftstücken, Plänen und Zeichnungen in Form von Dateien, wie sie mit den entsprechenden Erstellungs- und Bearbeitungsprogrammen erzeugt werden können. Solche Dateien werden entweder als sogenannte Attachments gemeinsam mit E-mails versandt, oder aber mit Hilfe anderer Übertragungstechniken übermittelt. Sie können weiters auch auf Datenträger gespeichert, und auf konventionellem Weg zu den Adressaten transportiert werden.

Die Übermittlung elektronischer Versionen von Dokumenten bietet vielfältige Vorteile. Einerseits erfolgt die Übermittlung selbst mit der Geschwindigkeit des Internet, sie steht als „unmittelbare" Funktion zur Verfügung, weiters bietet sie die Möglichkeit, dass der Adressat den Inhalt der elektronischen Version der Dokumente mit den entsprechenden Programmen nicht nur zur Darstellung bringen, sondern auch bearbeiten kann. Dies ist allerdings nicht immer gewünscht, sodass entsprechende technische Methoden dafür sorgen müssen, dass die Veränderung von Dokumenten durch den Adressaten, aber auch durch Fehler oder Manipulationen hintangehalten bzw. jedenfalls kenntlich gemacht werden. Mit der elektronischen Übermittlung von Dokumenten treten in diesem Zusammenhang Anforderungen an den Schutz der Dokumente auf, die durchaus in Analogie zum Versand herkömmlicher Dokumente angesehen werden können. Die Dokumente sollen auf dem Transportweg gegen Einsichtnahme durch Dritte gleichermaßen geschützt werden wie gegen unzulässige Veränderungen, weiters soll für den Empfänger die Herkunft des Dokuments, also der Absender deutlich erkennbar sein und darüber hinaus soll der Absender über eine gesicherte Möglichkeit verfügen die Zustellung eines Dokumentes verifizieren zu können. Für herkömmliche Dokumente und deren Versand bestehen dafür etablierte Verfahren, die beispielsweise in den Einschluss der Dokumente in Kuverts und der Versiegelung bestehen, sowie in dem Versand durch eingeschriebene Briefe mit Rückbestätigung. Solche Verfahren sind mit anderen technischen Methoden auch für elektronische Dokumente zu implementieren, wobei sich dabei zum Teil gegenüber den herkömmlichen Methoden erhebliche Qualitätsverbesserungen ergeben. Ein Beispiel dafür ist die Sicherstellung der Provenienz des Absenders, die bei einem herkömmlich versandten Schriftstück nicht unmittelbar gegeben ist.

Der vorliegende Artikel bietet eine Übersicht über die Methoden Dokumente im Zusammenhang mit ihrer elektronischen Übermittlung zu schützen und einen Ausblick auf zukünftige Entwicklungen.

2. Dokumente

Als Dokumente bezeichnet man Darstellungen, in der Regel in Form von Schriftstücken oder Graphiken. Sie stellen Urkunden dar, bei denen meist der Inhalt und in der Regel auch der Verfasser und der Zeitpunkt der Erstellung von Bedeutung sind. Sind Urkunden in entsprechender Form ausgefertigt, beispielsweise unterschrieben oder auch notariell beglaubigt, können sie in rechtlicher Hinsicht weitergehende Wirkung haben als wenn dies nicht der Fall ist.

Meist versteht man unter Dokumenten einfach Schriftstücke, die eine bestimmte Information enthalten. Solche Dokumente, unabhängig davon, ob sie nun lediglich Texte oder auch Graphik enthalten, können üblicherweise mit den Sinnesorganen des Betrachters interpretiert werden. Es wird dabei unmittelbar deutlich, welchen Inhalt das Dokument trägt und meist auch wer es verfasst bzw. unterfertigt hat und welche Datums- bzw. Zeitinformation dazu angefügt ist. Eine Verifikation dieser Informationen in Hinblick auf die Echtheit ist durch einfache Betrachtung in der Regel nicht möglich und kann sich häufig als äußerst schwierig erweisen. Oft sind dazu graphologische Gutachten und chemische Analysen zur Altersbestimmung erforderlich.

Bei der elektronischen Version von Dokumenten handelt es sich um eine Informationsmenge, die üblicherweise in einer Datei gespeichert wird, aus der sich das graphische Bild des Dokumentes ableiten lässt. Es kann damit zur Anzeige gebracht bzw. auch ausgedruckt werden. Dazu sind entsprechende Computerprogramme erforderlich, deren Art sich im Wesentlichen am Inhalt der Dokumente orientiert. Dokumente die aus Texten bestehen können dementsprechenden mit Textbearbeitungsprogrammen erstellt und wiederum zur Anzeige gebracht werden, für Dokumente die Bilder oder Zeichnungen, oder gemischte Inhalte aufweisen, sind andere Programme, wie Bildanzeigeprogramme, Dokumentendarstellungsprogramme, etc., erforderlich. Dokumente können mit solchen Programmen primär erstellt werden, gleichermaßen kann aber auch aus einem ursprünglich in konventioneller Form entstandenen Dokument, durch den Vorgang des Scannens eine elektronische Version erzeugt werden. Aus der Sicht der Informationstheorie stellt die elektronische Version eines Dokumentes eine Transformation des Informationsinhaltes, den das konventionelle Dokument enthält, dar. Der Vorgang der Wiedergabe und des Ausdrucks eines elektronischen Dokumentes stellt demnach die Überführung einer Informationsdarstellung in einen andere dar.

Beim Scannen einer graphischen Darstellung, also bei einer Digitalisierung, geht allerdings Information verloren. Der Grad des Informationsverlustes hängt dabei von der sogenannten Auflösung, das sind im Wesentlichen die Punktrasterung, und der Farbtiefe, das ist die Anzahl der dargestellten Farben, ab. Information die bei diesem Vorgang verloren geht, kann in weiterer Folge nicht mehr exakt wieder hergestellt werden. Dementsprechend muss darauf geachtet werden, dass ein Dokument so digitalisiert wird, dass jene Information, die für den Zweck des Dokumentes wichtig ist, erhalten bleibt. Wegen der bei der elektronischen Speicherung von Dokumenten anfallenden hohen Datenmengen werden zur Speicherung technische Verfahren verwendet, mit denen die erforderliche Informationsmenge minimiert werden kann. Ein einfaches Beispiel stellt die Speicherung von Texten dar. Es wird dabei lediglich gespeichert um welche Buchstaben bzw. welches Symbol aus dem Alphabet es sich handelt, während die graphische Ausführung, die bestimmt wie die einzelnen Buchstaben tatsächlich in der Anzeige dargestellt werden, genormt und weltweit verbreitet ist, sodass diese Information mit dem Dokument nicht gespeichert werden muss. Dadurch ist es auch möglich, ein und denselben Text in unterschiedlichen Schriftarten darzustellen. Dies kommt natürlich einer Veränderung des Aussehens eines ursprünglichen Dokumentes gleich.

Bei der Speicherung von Bildern werden sogenannte Kompressionsverfahren verwendet. Sie fußen darauf, dass nicht jeder Bildpunkt entsprechend der darzustellenden Auflösung des Bildes gespeichert werden muss, sondern dafür eine wesentlich geringere Zahl ausreicht. Der graphische Verlauf zwischen den Bildpunkten wird bei der Anzeige durch rechnerische Verfahren, wie beispielsweise Interpolationen, näherungsweise ermittelt. Dadurch kann bei der Speicherung der Bilder eine große Datenmenge eingespart werden. Die Darstellung des Bildinhaltes verändert sich allerdings durch die Anwendung dieser Verfahren. Die Art und Weise der Darstellung von Dokumenten ergibt sich aus Normen und Industriestandards. Sie sind im Bereich der PC-Technik aus den Dateiformaten und den Endungen der Dateien ersichtlich. Nachstehend sind einige wichtige Formate festgehalten.

Textformate

- TXT — ASCII Textfile (ohne Formatierung)
- DOC — WORD
- WPD — WordPerfect
- RTF — Rich Text Format

Graphik

- PSD — Adobe Photo Shop
- DXF — AutoCAD Drawing Exchange
- BMP — Windows Bitmap
- GIF — Graphics Interchange Format
- JPG — JPEG/JFIF Format
- TIFF — Tag Image File Format
- WMF — Windows Meta File Format

Zur Beschreibung von Dokumenten von gemischtem Inhalt stehen auch komplexere Formate zur Verfügung, mit denen zum Teil auch Strukturen vorgegeben und Inhaltsklassen definiert werden können. Die wichtigsten Formate dazu sind.

- PDF — Portable Document Format
- HTML — HyperText Markup Language
- XML — Extensible Markup Language

Dateiformate können häufig neben Informationen, die unmittelbar zur Darstellung verwendet werden, auch Programmzeilen enthalten, die bei der Darstellung des Dokumentes als Programm ausgeführt werden. Beispiele dafür sind sogenannte Makros in Word Dokumenten, mit denen die Darstellung des Dokumentes gesteuert verändert werden kann. Dadurch kann auch ein Dokument erstellt werden, das abhängig vom Systemdatum eines Computers unterschiedliche Texte oder Zahlenwerte zur Anzeige bringt.

Es ist jedenfalls erforderlich, dass man sich des Umstandes bewusst wird, dass völlig unabhängig von der Absicherung der Dokumente gegen Verfälschung mit Hilfe elektronischer Signaturen, wie sie im weiteren beschrieben werden, sich die „Echtheit" eines elektronischen Dokumentes ausschließlich auf die elektronisch gespeicherte Form, die mit den Sinnesorganen allerdings nicht interpretierbar ist, beziehen kann. Diese elektronische Form enthält beispielsweise bei Bildern nur eine geringe Anzahl „echter" Bildpunkte, die überwiegende Anzahl wird bei der Darstellung durch Rechenvorgänge rekonstruiert. Sie stellen lediglich eine Annäherung – nicht definierter Genauigkeit – an

eine allenfalls zuvor vorhandene „echte" Vorlage dar. Der Ausdruck bzw. die bildliche Darstellung eines elektronischen Dokumentes stellt daher lediglich eine Kopie bzw. aus technischer Sicht eine Transformation des elektronischen Dokumentes dar, die je nach verwendetem Hilfsmittel zur Herstellung unterschiedlich aussehen kann. „Echt" ist in diesem Fall die elektronische Version. Während aus technischer Sicht die Bestrebung zweckmäßig ist, Dokumente mit zukünftigen Techniken für Anzeigeprogramme in verbesserter Qualität darstellen zu können, wird das Ziel rechtlicher Anforderungen an solche Systeme darin bestehen müssen, unabhängig von der Technologie, dafür zu sorgen, dass die Darstellung elektronischer Dokumente immer gleich aussieht.

3. Der Schutz von Dokumenten

3.1 Allgemeines

Bei der Übermittlung von elektronischen Dokumenten besteht das, je nach Anwendung unterschiedlich stark ausgeprägte, Erfordernis die Echtheit des Inhaltes und des Versenders abzusichern. Nachstehende Eigenschaften sind dabei von Bedeutung.

Vertraulichkeit

Ein wesentlicher Begriff bei der Informationsübermittlung ist die Vertraulichkeit des übertragenen Inhalts. Es soll sichergestellt werden, dass nur jene Personen, für die die Nachricht bestimmt ist, diese auch lesen können. Es muss dazu ein Schutz gegen den Zugriff auf den Dokumenteninhalt durch Dritte implementiert werden. Dazu stehen die Methoden der Verschlüsselung zur Verfügung.

Integrität

Darüber hinaus besteht auch das Erfordernis die Unverfälschtheit des Dokumenteninhaltes zu sichern. Wie vorstehend dargestellt, können elektronische Dokumente mit Hilfe der zugehörigen Erstellungsprogramme verändert werden, sodass am Wege der Übermittlung die Möglichkeit bestehen kann den Inhalt von Dokumenten zu verfälschen. Der dazu erforderliche Schutz ist unabhängig von einer allfälligen Verschlüsselung des Inhalts, die das Dokument für Dritte unlesbar macht. Es ist auch für nicht verschlüsselte Dokumente sicherzustellen, dass Änderungen nicht möglich bzw. unmittelbar kenntlich gemacht werden. Die technische Lösung zur Sicherstellung der Integrität stellt die Verwendung elektronischer Signaturen dar.

Authentizität

Dabei handelt es sich um die Zuordnung eines elektronisch übermittelten Dokumentes zu einem Absender. Eine einfache Lösung dafür besteht darin, das Dokument einer technischen Adresse zuzuordnen. Dabei kann es sich beispielsweise um die Emailadresse eines Versenders handeln. Ohne weitere technische Maßnahmen besteht beim üblichen Emailversand die sehr einfache Möglichkeit der Fälschung einer Absenderadresse. Zur sicheren Zuordnung einer Nachricht zu einer Absenderadresse sind weitere Maßnahmen, die ebenfalls durch die Verwendung elektronischer Signatur geboten werden, erforderlich. Allerdings muss der Empfänger dabei auch eine gesicherte Kenntnis darüber haben, wer der Inhaber der zugeordneten Emailadresse ist. Meist kann nicht einfach verifiziert werden, ob die Versendung tatsächlich durch den Inhaber oder allenfalls im Rahmen eines Mißbrauchs erfolgt ist. Eine weitergehende Anforderung besteht darin, ein Dokument einer Person zuordnen zu können. Dazu ist neben der Zuordnung zu einer technischen Adresse auch noch eine Verknüpfung der Adresse mit der Person erforderlich. Dies wird ebenfalls durch Verwendung elektronischer Signaturen erreicht, wobei die Zuordnung der technischen Adresse zur Person durch Institutionen bestätigt werden, die mit einer Art des öffentlichen Vertrauens ausgestattet sind. Dazu muss sich der Inhaber einer solchen Adresse bei diesen Institutionen registrieren lassen, sich in der Regel persönlich legitimieren und die Zuordnung autorisieren. Er erhält dabei eine technische Einrichtung, beispielsweise in Form einer Chipkarte, die es ausschließlich ermöglicht die ihm zugeordnete Signatur herzustellen. Er muss allerdings selbst dafür sorgen, dass diese Chipkarte nicht mißbräuchlich verwendet wird.

3.2 Kryptographie

3.2.1 Grundlagen

Das Grundprinzip der Verschlüsselung von Nachrichten, ist schon lange bekannt und wird, seitdem Nachrichten zwischen Menschen ausgetauscht werden, in der einen oder anderen Art verwendet. Das nachstehende Bild zeigt das Grundprinzip der sogenannten symmetrischen Verschlüsselung, bei der der Versender und der Empfänger jeweils den gleichen Schlüssel zum entschlüsseln und verschlüsseln verwenden.

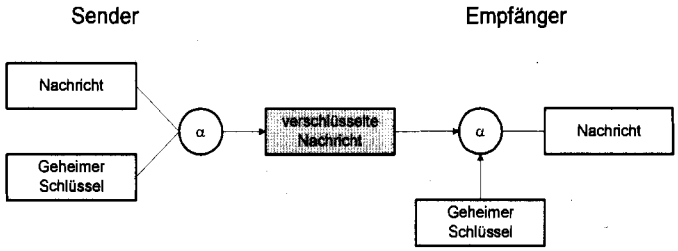

Bild 1: Symmetrische Verschlüsselung

Die zu verschlüsselnde Nachricht wird dabei beim Sender mit dem Schlüssel in einer Art und Weise – meist rechnerisch – verknüpft, die beim Empfänger durch eine reziproke Operation rückgängig gemacht werden kann. Dieses System setzt voraus, dass Sender und Empfänger einander kennen, bzw. zumindest über den gleichen Schlüssel verfügen, der zuvor in irgend einer Art und Weise ausgetauscht werden muss. Diese Art der Verschlüsselung eignet sich dementsprechend nicht für den Informationsaustausch zwischen Personen die zuvor miteinander nicht Kontakt hatten, da als erster Schritt ein entsprechend gesicherter Schlüsselaustausch erfolgen müsste. Jedenfalls muss der verwendete Schlüssel geheim gehalten werden.

Eine Lösung für dieses Problem bilden die sogenannten asymmetrischen Verschlüsselungsverfahren, bei denen der Sender und der Empfänger unterschiedliche Schlüssel verwenden. Das Grundprinzip ist im nachstehenden Bild dargestellt. Es basiert darauf, dass es bei Anwendung entsprechender mathematischer Verfahren, die der Sender und der Empfänger benutzen, gelingt zur Verschlüsselung einen Schlüssel zu verwenden, mit dem es nach der einmal durchgeführten Verschlüsselung nicht mehr gelingt, die verschlüsselte Nachricht wieder zu entschlüsseln. Zur Entschlüsselung ist ein zweiter Schlüssel erforderlich, der zu jenem Schlüssel mit dem verschlüsselt wurde, passen muss.

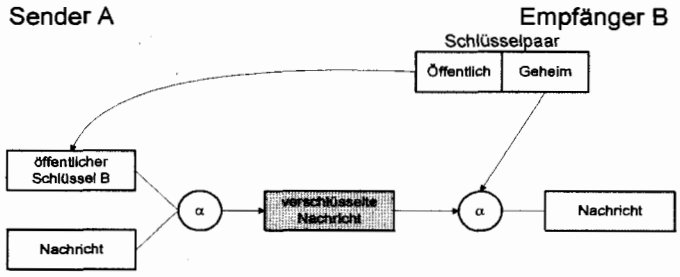

Bild 2: Asymmetrische Verschlüsselung, Public Key Systeme

Zur Anwendung dieses Systems muss ein Empfänger, der eine verschlüsselte Nachricht erhalten will, über die beiden Schlüssel verfügen. Sie werden als Schlüsselpaar in einem technischen Vorgang erzeugt. Jener Teil mit dem verschlüsselt werden soll, wird allen möglichen Empfängern zugängig gemacht, er wird daher als öffentlicher Schlüssel bezeichnet. Jeder kann diesen Schlüssel verwenden und auf diese Art und Weise eine Nachricht verschlüsseln, die an den Adressaten gerichtet ist. Da sich mit dem öffentlichen Schlüssel verschlüsselte Nachrichten mit diesem Schlüssel nicht mehr entschlüsseln lassen, verfügt niemand außer dem Empfänger über die Möglichkeit die Nachrichten zu entschlüsseln. Dazu benötigt er den zweiten Teil des Schlüsselpaares, den man als geheimen Schlüssel bezeichnet. Mit ihm ist es möglich, mit einer entsprechenden Rechenoperation die verschlüsselte Nachricht wieder in die Klartextnachricht umzuwandeln.

Zur Realisierung der asymmetrischen Verschlüsselungsverfahren stehen unterschiedliche mathematische Methoden zur Verfügung. Der bekannteste Algorithmus ist der sogenannte RSA Algorithmus *(Rivest, Shamir, Adlemann)*. Die mathematischen Grundlagen lassen sich wie folgt einfach darstellen.

Nachricht m	{0 - (n-1)}
Geheimtext c	{0 - (n-1)}
öffentlicher Schlüssel e	{0 - n} (e,n)
geheimer Schlüssel d	{0 - n} (e,n)

Bedingungen für das Schlüsselpaar

$n = p * q$	n ... nat. Zahl
$Z = (p-1)*(q-1)$	p, q ... Primzahlen
$e * d = k * (p-1)(q-1) + 1$	k ... nat. Zahl
$(d * e) \bmod z = 1$	

Verschlüsseln	$c = m^e \bmod n$
Entschlüsseln	$m = c^d \bmod n$

Ein vertieftes Verständnis für den Vorgang kann man auf einfache Weise dadurch gewinnen, dass man das Verfahren mit „kleinen" Zahlen nachprüft. Dazu kann man beispielsweise für die beiden Primzahlen p und q die Werte 3 und 11 auswählen und auf diese Weise z (es ergibt sich die Zahl 20) errechnen.

Ein Schlüsselpaar lässt sich entsprechend der angegebenen Gleichung durch Probieren leicht finden, sodass dem Versuch, beispielsweise die Textnachricht m=3 zu verschlüsseln und das Ergebnis weiters wieder zu entschlüsseln kein Hindernis im Wege stehen sollte. Reale Schlüsselpaare verwenden lange Binärzahlen, sodass das Probieren zur Ermittlung des einen Schlüssels aus dem anderen so rechenaufwendig ist, dass dies mit den bestehenden Computern in einer praktikablen Zeit nicht ausgeführt werden kann.

3.2.2 Digitale Signatur

Die digitale Signatur ist ein Kennzeichen, das einen Schluss auf die Unverfälschtheit der signierten Daten zulässt. Wenn in diese Daten nicht nur eine zu übermittelnde Datei, sondern auch Informationen über den Absender, beispielsweise in Form einer technischen Adresse, einbezogen werden, kann damit auch eine Zuordnung einer empfangenen Nachricht zu dieser Absenderadresse vorgenommen werden.

Zur Herstellung einer digitalen Signatur, also des Kennzeichens mit dem die Unverfälschtheit einer übermittelten Nachricht samt Absenderinformation gewährleistet wird, werden die Methoden der asymmetrischen Verschlüsselung, wie vorstehend beschrieben, angewandt. Man nützt dabei die Eigenschaft dieser Verfahren aus, dass sich sowohl der öffentliche als auch der geheime Schlüssel dafür eignen eine Nachricht zu verschlüsseln und jeweils der andere Teil des Schlüssels dann zum entschlüsseln verwendet werden kann. Das Grundprinzip der Erzeugung einer Signatur ist im nachstehenden Bild widergegeben. In einem ersten Schritt wird für das Dokument für das eine Signatur erzeugt werden soll, ein sogenannter Hash Wert gebildet. Dabei handelt es sich um die Berechnung einer Zeichenkette, die auf dem Inhalt der Datei fußt und für diese Datei repräsentativ ist. Dafür stehen unterschiedliche Verfahren zur Verfügung, beispielsweise kann für eine Datei, für die eine Signatur erstellt werden soll, ein Hash Wert, der eine Länge von 160 Stellen hat, erzeugt werden. Geht man von einer Datei aus und erzeugt einen Hash Wert, ergibt das mathematische Verfahren, dass jede Änderung an der Datei dazu führt, dass ein anderer Hash Wert generiert wird. Das Prinzip dieser Kennzeichnung fußt darauf, dass praktisch keine zwei Nachrichten erzeugt werden können, bzw. eine Nachricht nicht so verfälscht werden kann, dass sich bei der Berechnung des Hash Wertes jeweils der gleiche Wert ergibt.

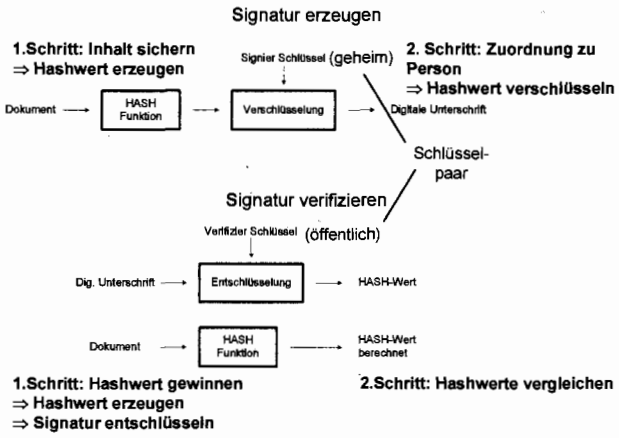

Bild 3: Elektronische Signatur

Der für das Dokument gebildete Hash Wert wird im Zuge des Signierens eines Dokumentes mit dem geheimen Schlüssel der Person, die die Signatur erzeugt, verschlüsselt. Dies ist jener Schlüssel über den nur diese Person verfügt. Die verschlüsselte Version des Hash Wertes stellt die digitale Unterschrift dar. Sie ist durch die Verwendung des Hash Wertes, sowohl für das Dokument als auch durch die Verwendung des geheimen Schlüssels für die unterfertigende Person signifikant.

Zur Überprüfung der Echtheit und Unverfälschtheit des Dokumentes sind beim Empfänger zwei Schritte erforderlich. Das Grundprinzip basiert darauf, dass für das empfangene Doku-

ment beim Empfänger ebenfalls der Hash Wert gebildet wird. Dieser Hash Wert wird mit jenem verglichen, der sich aus der digitalen Signatur – die den Hash Wert verschlüsselt enthält – nach der Entschlüsselung ergibt. Zur Entschlüsselung der digitalen Signatur ist der öffentliche Schlüssel des Signators, das ist jene Person die die Unterschrift erzeugt hat, erforderlich. Stimmen die beiden Hash Werte, nämlich jener der sich aus dem Dokument selbst ableiten lässt und jener der sich aus der Entschlüsselung der Signatur ergibt, überein, ist das Dokument als unverfälscht und dem Signator zuzuordnen anzusehen.

Dadurch erfolgt allerdings noch keine Bindung an eine bestimmte Person. Im allgemeinen Fall kann der Empfänger einer Nachricht sich wohl den öffentlichen Schlüssel eines Versenders, der eine Nachricht signiert hat, beschaffen, beispielsweise von einer WEB Seite oder einem sogenannten Schlüsselserver, er kann allerdings nicht wissen, ob der vermutete Versender tatsächlich der Ersteller und Inhaber dieses Schlüssels ist. Um eine sichere Zuordnung zu einer Person vornehmen zu können, muss eine Zuordnung des verwendeten öffentlichen Schlüssels – der im Zuge des Entschlüsselungsvorganges einen Rückschluss darauf zulässt, dass nur der Besitzer des zugehörigen geheimen Schlüssels der Signator sein kann – vorgenommen werden.

Dazu stehen im praktischen Geschäftsleben mehrere Möglichkeiten zur Verfügung. Die einfachste Möglichkeit besteht darin den öffentlichen Schlüssel einer Person, die ein signiertes Dokument übersendet, von dieser Person direkt zu erhalten, oder aber von einer Quelle zu beziehen, für die die allenfalls auch persönlich bekannte Person vertrauenswürdig bestätigt, dass es sich dabei um den eigenen öffentlichen Schlüssel handelt. Im praktischen Geschäftsleben wird so eine Zuordnung eines öffentlichen Schlüssels zu einer Person, beispielsweise durch ein Telefonat, oder dadurch, dass der öffentliche Schlüssel auf der WEB Seite des Versenders enthalten ist, ausreichen, um eine Personenzuordnung mit ausreichender Sicherheit annehmen zu können.

Im allgemeinen Fall ist allerdings der Personenkreis der Signatoren von Dokumenten untereinander nicht bekannt, sodass zur Zuordnung von öffentlichen Schlüsseln zu Personen sogenannte Zertifikatsdienste herangezogen werden. Dabei handelt es sich um Einrichtungen, die im Rahmen gesetzlich definierter Kontroll- und Aufsichtsmaßnahmen tätig, und somit per Definition vertrauenswürdig sind und als sicher gelten. Diese Institutionen verwenden eigene Schlüssel, mit denen sie die – verifizierte – Zuordnung des unterschriebenen Schlüssels mit einer Person bestätigen.

3.2.3 Technische Aspekte

Für die technische Umsetzung der kryptographischen Verfahren, sind wesentliche Parameter durch die die Sicherheit beeinflusst werden, zu beachten. Eine wesentliche Rolle spielen dabei die Verfahren zur Herstellung des Hash Wertes und die Schlüssellänge, die im Verschlüsselungs- bzw. Signiervorgang verwendet werden. Im Allgemeinen gilt, dass mit der Länge des Hash Wertes und der Schlüssellänge die Sicherheit bzw. der Aufwand um eine unautorisierte Dechiffrierung durchführen zu können steigt. Praktisch gesehen werden die Werte dabei so gelegt, dass mit aktuellen Technologien eine unautorisierte Entschlüsselung, wegen der dabei auftretenden langen Rechenzeiten, nicht möglich ist. Daraus ergibt sich auch, dass Schlüssellängen und auch Verschlüsselungsverfahren nur für einen bestimmten Zeitraum als sicher angenommen werden. Nach Verstreichen dieses Zeitraumes muss die Situation, auf Basis der dann zur Verfügung stehenden technologischen Möglichkeiten, jeweils neu bewertet und allenfalls verbesserte Verfahren oder längere Schlüssel eingesetzt werden.

Eine weitere wesentliche Implementierungsfrage besteht darin, wo der geheime Schlüssel, der zur Entschlüsselung bzw. zum Signieren erforderlich ist, gespeichert wird und wo der Veschlüsselungsvorgang, das ist eine Menge von Rechenoperationen, tatsächlich ausgeführt wird. Speichert man beispielsweise den geheimen Schlüssel in einem Personalcomputer und führt die Rechenvorgänge zum Verschlüsseln bzw. zum Signieren mit der CPU des Personalcomputers aus, ergibt sich das Problem, dass der Schlüssel allenfalls unautorisiert aus diesem Computer ausgelesen bzw. von nicht autorisierten Personen verwendet werden kann. Alternativ dazu können zur Erstellung der Signatur – man spricht von Signaturerstellungseinheiten – anstelle des Personalcomputers Chipkarten, auf denen auch Prozessoren enthalten sein können, verwendet werden. Auf diesen Chipkarten kann auch der geheime Schlüssel gespeichert werden, wobei gleichzeitig spezielle Schutzmechanismen dafür sorgen, dass der geheime Schlüssel aus der Chipkarte nicht ausgelesen werden kann. Schützt man weiters die Chipkarte durch Verwendung eines PIN Codes gegen unautorisierte Verwendung, wird mit hoher Sicherheit gewährleistet, dass lediglich die autorisierte Person mit dem geheimen Schlüssel signieren und dass dieser Schlüssel nicht dupliziert werden kann.

4. Anwendung elektronischer Signaturen

Im Bürobereich können unterschiedliche Ausführungsformen elektronischer Signaturen eingesetzt werden. Überall dort, wo die Speicherung des geheimen Schlüssels in einem Computer für die zu erreichende Sicherheit ausreicht, können sogenannte „Softsignaturen" verwendet werden. Dies ist beispielsweise oft in Büroumgebungen der Fall in denen durch organisatorische Maßnahmen sichergestellt ist, dass Fremde weder Zutritt zu den Personalcomputern der einzelnen Personen haben, noch ein unautorisierter Auslesevorgang eines Schlüssels stattfinden kann. Geht man im Geschäftsverkehr davon aus, dass der Schlüsselaustausch zwischen den Beteiligten durch persönliche Übermittlung oder Bestätigung, oder durch Kennzeichnung auf WEB-Seiten zur Zuordnung eines Schlüssels zu einer Person ausreicht, muss auch kein Zertifikatsdienst involviert werden.

Ein weit verbreitetes Softwareprodukt, das diese Anforderungen abdeckt, ist das Produkt PGP (Pretty Good Privacy). Dabei handelt es sich um ein Computerprogramm, das auch in WINDOWS und MS-Office-Umgebungen betrieben werden kann. Es erlaubt die Generierung von Schlüsselpaaren und ihre Verwaltung und verfügt über Funktionen, um Emails und einzelne Dateien zu signieren sowie diese und gesamte Festplattenbereiche mit Hilfe asymmetrischer Verfahren zu verschlüsseln. Bei der Versendung eines E-mails prüft das System beispielsweise automatisch, ob der öffentliche Schlüssel des Adressaten bereits gespeichert ist und führt den Verschlüsselungsvorgang gegebenenfalls automatisch durch. Bei ankommenden verschlüsselten E-mails kann das System so betrieben werden, dass eine automatische Entschlüsselung erfolgt.

Systeme, bei denen erhöhte Sicherheitsanforderungen gelten, involvieren Schlüssel für die Zertifikate von Zertifikatsdienstanbietern vorliegen, mit Hilfe derer die aktuelle Gültigkeit des Schlüssels und die Zuordnung zu einer Person verifiziert werden können.

Eine weitere Verbesserung der Sicherheit ergibt sich durch die Verwendung von Chipkarten, in denen die Zertifikate gespei-

chert sind. Mit Hilfe entsprechender Softwareteile können in Office-Umgebungen einfache Lesegeräte, in die solche Chipkarten eingeschoben werden, angesprochen werden.

Das Signaturgesetz sieht vor, dass die elektronische Unterschrift gewisse Rechtswirkungen dann entfaltet, wenn sie bestimmten technischen Ausführungs- und Umfeldbestimmungen entspricht. Dazu ist es erforderlich, dass die verwendeten Komponenten von entsprechend autorisierten Stellen überprüft und bestätigt sind. Eine besondere Stellung kommt dabei, neben den Chipkarten selbst, auch jenen Programmen zu, mit denen ein Dokument im Zuge der Erstellung einer Signatur angesehen und validiert werden kann und weiters die Gültigkeit einer Signatur beim Empfänger überprüft werden kann. Dabei handelt es sich um die sogenannten „Secure Viewer". Diese Programme stellen sicher, dass Dateien, für die Signaturen erstellt werden, sowohl bei der Erstellung der Signatur als auch später, in der gleichen Art und Weise interpretiert und zur Anzeige gebracht werden. Hält man sich die technischen Methoden zur Speicherung von Texten und Graphiken vor Augen sowie weiters auch die Möglichkeiten, beispielsweise in Word Dokumente sogenannte Makros einzubauen, die automatisch das Erscheinungsbild und auch den dargestellten Inhalt einer Datei verändern können, muss ein derartiger Viewer sicherstellen, dass eine Datei keine Elemente aufweist, die eine solche automatische Veränderung zulassen. Weiters muss sichergestellt werden, dass die verwendeten Komprimierungsverfahren bei der Anzeige jeweils in gleicher Art und Weise aufgelöst werden und zum gleichen graphischen Ergebnis führen. Diese Anforderung führt dazu, dass solche Viewer nur für eine geringe Anzahl von Datenformaten, wie beispielsweise XML, vorliegen und vielfältige Formate, die mit weit verbreiteten Textverarbeitungsprogrammen erzeugt werden können, nicht mit sicheren Signaturen signiert werden können. Unabhängig davon besteht die Möglichkeit, bei der Übermittlung der elektronischen Version eines Dokumentes, durch die Verwendung einer Signatur, die Authentizität und Integrität der Datei zu sichern und damit dafür zu sorgen, dass unautorisierte Änderungen erkennbar sind.

Auch die ledigliche Absicherung der elektronischen Form eines Dokumentes, ohne Einbeziehung seiner visuellen Darstellung, ist vielfach aus praktischer Sicht zweckmäßig. Man kann damit nachweisen, in welcher Art und Weise mit welcher Zeit- und Datumskennung man eine Datei, beispielsweise eine Textdatei, an jemand anderen übergeben hat. Würde später eine veränderte Datei als zugegangen behauptet werden, ließe sich mit Hilfe der Signatur leicht der Nachweis erbringen, dass es sich um eine manipulierte Datei handelt. Wenngleich diese Anwendungen digitaler Signaturen hohe praktische Bedeutung im Geschäftsleben haben, entspricht dies nicht den Vorgaben des Signaturgesetzes an die Ausführung einer sicheren Signatur, in die jedenfalls auch die Darstellung des signierten Dokumentes in bestätigter Art und Weise einbezogen wird.

5. Ausblick

Durch das Signaturgesetz und die Signaturverordnung, sowie weiters auch durch das e-Government Gesetz, wird die Anwendung elektronischer Signaturen in ihrer „sicheren" Ausführung definiert und für wesentliche Geschäftsfälle des Verkehrs von Parteien mit den Behörden vorgesehen. Dazu sind Chipkarten mit sicheren Signaturen und einer Personenzuordnung erforderlich sowie weiters auch entsprechende Anwendungsprogramme und Applikationen, die die Verwendung dieser Signaturen entsprechend der gesetzlichen Vorgaben erlauben. Ein aktuelles Beispiel dafür, das für viele weitere Einsatzgebiete maßgebend sein wird, ist die elektronische Zustellung von Schriftstücken von Behörden mit einer entsprechenden Rechtswirkung im Sinne des Zustellgesetzes. Dabei ist vorgesehen, dass sich die Bürger eines sogenannten Zustelldienstes bedienen, gegenüber den man sich, gleichermaßen wie der Behörde gegenüber, mit Hilfe einer sicheren elektronischen Signatur identifizieren muss. Nach einer entsprechenden Verständigung per E-mail und Identifikation dem Zustelldienst gegenüber hat man die Möglichkeit das Behördenschriftstück, das von der Behörde auch signiert ist, auf seinen Computer zu laden. Ein derartiges, von der Behörde signiertes, Schriftstück kann auch, da dadurch die Authentizität gewährleistet ist, auf elektronischem Wege wiederum der Behörde vorgelegt werden. Vorgesehen ist dabei auch die zentrale Speicherung der wesentlichen Schriftstücke die man üblicherweise im Verkehr mit den Behörden benötigt.

Für den Kreis der Gerichtssachverständigen wird eine entsprechende elektronische Signatur zur Authentifizierung der Justiz gegenüber verwendet werden. Sie wird auf Chipkarten enthalten sein, die entsprechend dem Sachverständigen- und Dolmetschergesetz als Sachverständigenausweise ausgegeben werden. Mit Hilfe dieser Signatur können die Sachverständigen spezielle Daten der elektronisch geführten Sachverständigenliste auch selbst warten. Der weitere Automatisierungsschritt der elektronischen Übermittlung von Gutachten auf Basis einer vorgegebenen Struktur und einer elektronischen Unterschrift, stellt dabei einen logischen Schritt dar, der vorhergesehen werden kann.

Für übliche Office-Anwendungen im Geschäftsleben sowie allenfalls auch für Informationsübermittlungen zu Behörden, für die nicht so hohe Sicherheitsanforderungen bestehen, ist auch eine weniger qualifizierte Signatur ausreichend. Dabei kann es sich entweder um einfache Signaturen oder sogenannte fortgeschrittene Signaturen oder Verwaltungssignaturen handeln. Zur Anwendung im üblichen Geschäftsleben werden dabei zum überwiegenden Teil auch computerbasierte Signaturen und Softzertifikate ausreichen, die den Sicherheitsstandard bei der Übermittlung von Informationen, gegenüber nicht signierten Verfahren signifikant erhöhen. Ihre Anwendung ist einfach, eine wesentliche Verbreitung dieser Techniken und zugehöriger Produkte in absehbarer Zeit kann vorhergesehen werden. Festgehalten kann zur Anwendung dieser Techniken auch werden, dass sich auch schon durch die Verwendung einfacher Signaturen bei der elektronischen Informationsübermittlung der Sicherheitsstandard gegenüber der Übermittlung konventioneller Dokumente erheblich verbessert. Durch die elektronische Unterschrift kann der Versender identifiziert werden, die technischen Fälschungsmöglichkeiten sind gering bzw. erheblich aufwendiger als dies bei Schriftstücken der Fall ist.

Literatur:

Smith, Richard E.: Internet-Kryptographie, Bonn: Addison-Wesley-Longmann, 1998
Brenn, C.: Signaturgesetz: SigG; Bundesgesetz BGBl I 1999/190, Wien Manz, 1999
Brenn, C., Posch R.: Signaturverordnung, Wien: Manz, 2000
Born, G: Dateiformate – Die Referenz, Bonn: Galileo Press GmbH, 2001

Korrespondenz:
Prof. Dipl.-Ing. Dr. Kurt P. Judmann
Judmann Ziviltechniker GmbH
A-1040 Wien, Rechte Wienzeile 5/2
E-mail: k.judmann@jic.at