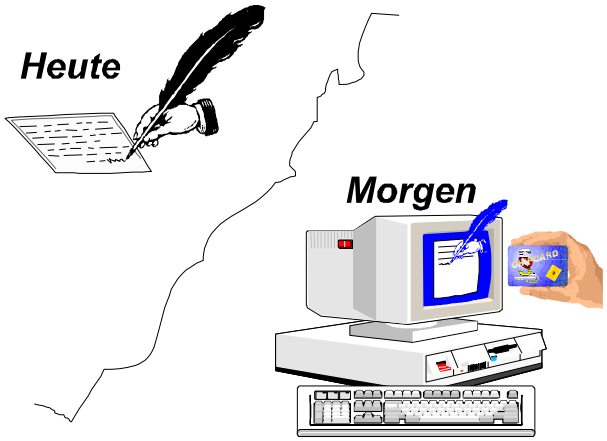

Digitale Signatur nach dem deutschen Signaturgesetz

1. Bedeutung der digitalen Signatur

Die Entwicklung der Informations- und Kommunikationstechnik eröffnet neue Möglichkeiten des Informationsaustausches und der wirtschaftlichen Betätigung. Warenbestellungen, Zahlungsanweisungen an Banken, Anträge oder Einsprüche bei Behörden, die Übermittlung sensitiver Daten im medizinischen Bereich und eine Vielzahl weiterer Kommunikationsbeziehungen sowohl in formfreien als auch öffentlich-rechtlichen Bereichen, die in der Vergangenheit über Papier abgewickelt wurden, erfolgen bereits zu einem großen Teil auf elektronischem Wege. Dies gilt auch für die Dokumentation von Daten, z.B. im Hinblick auf die Produkthaftung oder im Medizinbereich. Neu hinzu kommen multimediale Anwendungen.

Da sich die Dokumentationserstellung, Kommunikation und Archivierung auf der Basis digitaler Daten etabliert hat und expandiert, ergibt sich der dringende Bedarf nach einer digitalen Lösung, die den Anforderungen einer offenen Kommunikation (in der sich die Teilnehmer nicht kennen müssen) gerecht wird, bei der **zuverlässig auf den Urheber geschlossen werden kann und die Daten vor unbemerkter Veränderung geschützt sind**. Diese Forderungen erfüllt die gesetzliche digitale Signatur.

2. Funktionsweise der digitalen Signatur

Eine digitale Signatur ist eine Art von Siegel zu digitalen Daten. Es wird unter Einsatz mathematischer Verfahren mit Hilfe eines privaten kryptographischen Schlüssels erzeugt. Mit Hilfe des dazugehörigen öffentlichen Schlüssels kann die Signatur jederzeit überprüft und damit der Signaturschlüssel-Inhaber und die Unverfälschtheit der Daten festgestellt werden.

Die jeweils einmaligen Schlüsselpaare (privater und öffentlicher Schlüssel) werden durch anerkannte Stellen natürlichen Personen fest zugeordnet. Die Zuordnung wird durch ein Signaturschlüssel-Zertifikat beglaubigt. Es handelt sich dabei um ein signiertes „digitales Dokument“, das den jeweiligen öffentlichen Schlüssel sowie den Namen der Person, der er zugeordnet ist, oder ein Pseudonym enthält. Das Zertifikat erhält der Signaturschlüssel-Inhaber, so daß er es signierten Daten für deren Überprüfung beifügen kann. Darüber hinaus ist es über öffentlich erreichbare Telekommunikationsverbindungen jederzeit für jedermann nachprüfbar.

Der breite Einsatz von digitalen Signaturverfahren erfordert eine zuverlässige und effektive Sicherheitsinfrastruktur für die Zuordnung der Signaturschlüssel durch Zertifikate (Zertifizierungsstellen) sowie sichere technische Komponenten. Weiter müssen die Signaturschlüssel-Inhaber darüber unterrichtet sein, welche Maßnahmen sie in ihrem eigenen Interesse für sichere digitale Signaturen zu treffen haben.

3. Gesetz zur digitalen Signatur

Am 1. August 1997 ist das aus 11 Artikeln bestehende „Informations- und Kommunikationsdienste Gesetz“ durch den Deutschen Bundestag in Kraft gesetzt worden [IuKD97]. Dieses Gesetz beinhaltet in Artikel 3 das Gesetz zur digitalen Signatur (SigG). Die dazugehörige Verordnung zum Gesetz zur digitalen Signatur (SigV) wurde nach langer Diskussion abschließend am 1. November 1997 in Kraft gesetzt [SigV97]. Das Gesetz soll Rahmenbedingungen schaffen, bei deren Einhaltung eine digitale Signatur als mindestens gleichwertig sicher zu einer eigenhändigen Unterschrift angesehen werden kann. Bei entsprechender gesetzmäßiger Umsetzung wird dies zu weitreichenden Konsequenzen führen.

Damit ermöglicht das Gesetz für Wirtschaft und Verwaltung praktisch einen medienbruchfreien vollständigen Umstieg vom „Papierdokument“ auf das „elektronische Dokument“. Selbst beweiserhebliche Vorgänge können künftig vollständig elektronisch abgewickelt werden (z.B. Steuerdaten von der elektronischen Buchführung über den Steuerberater bis zum Steuerbescheid des Finanzamtes). Sowohl das Gesetz als auch die zugehörige Verordnung definieren weder detaillierte Vorgaben an die Organisation noch geben sie detaillierte technische Vorgaben. Sie lassen bewußt genügend Spielraum für zukünftige innovative Lösungen.

Gleichwohl lassen sich implizit aus den aus der Verordnung abgeleiteten Sicherheitsanforderungen und Maßnahmen konkrete Lösungen im Sinne von Sicherheitsfunktionalitäten ableiten. So zeigt etwa das vom Bundesamt für Sicherheit in der Informationstechnik in Zusammenarbeit mit Industrie, Wirtschaft und Wissenschaft erstellte Handbuch zur digitalen Signatur [BSI97] zu §§ 12(2) und 16(6) der Verordnung beispielhaft organisatorische und technische Leitvorgaben für Hersteller und Anwender auf.

4. Sicherheit digitaler Signaturen

- **Behördlich genehmigte Zertifizierungsstellen**

Die Zuordnung von Signaturschlüsseln (durch elektronische Zertifikate) für die Erzeugung gesetzlich anerkannter digitaler Signaturen bedarf der Genehmigung der „Regulierungsbehörde für Telekommunikation und Post“, die seit dem 1. Januar 1998 im Geschäftsbereich des Bundesministeriums für Wirtschaft untergebracht ist. Voraussetzung für die Erteilung einer Genehmigung ist, daß die Zertifizierungsstelle über die erforderliche Zuverlässigkeit und Fachkunde verfügt. Darüber hinaus muß eine von der Regulierungsbehörde anerkannte Stelle (Bestätigungsstelle) die Umsetzung der Vorgaben des Gesetzes (Sicherheitskonzept) geprüft und bestätigt haben. Die Signaturverordnung sieht vor, daß die Prüfung regelmäßig im Abstand von zwei Jahren sowie nach wesentlichen Veränderungen zu wiederholen ist. Darüber hinaus kann die Regulierungsbehörde stichprobenweise sowie bei begründetem Anlaß eigene Kontrollen durchführen.

- **Sicherheitsgeprüfte technische Komponenten**

Die technische Sicherheit der gesetzlich anerkannten digitalen Signaturen beruht vor allem auf folgenden technischen Faktoren:

- sichere kryptographische Verfahren,
- einmalige Signaturschlüsselpaare,
- zuverlässige Bindung der geheimen, privaten Signaturschlüssel an die rechtmäßigen Nutzer,
- Ausschluß nicht gewollter digitaler Signaturen,
- zuverlässige Nachprüfung der Gültigkeit von Zertifikaten.

Die Eignung der kryptographischen Verfahren für digitale Signaturen ist durch einen Kreis führender Kryptologen aus Wissenschaft, Wirtschaft und Behörden jährlich sowie nach Bedarf neu zu bestimmen. Es werden nur solche Verfahren zugelassen, wenn innerhalb des bestimmten Zeitraumes (mindestens sechs Jahre) nach dem Stand von Wissenschaft und Technik eine nicht feststellbare Fälschung von digitalen Signaturen oder Verfälschung von signierten Daten mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden kann. Dies schließt die Einmaligkeit der Signaturschlüssel ein, die bereits über die Verfahren zur Schlüsselerzeugung gewährleistet ist. Die vorgesehene Schlüssellänge beträgt z.B. beim „RSA-Verfahren“ zur Zeit 1024 Bit, was etwa einer 300-stelligen Zahl entspricht. Zusätzlich prüft die Zertifizierungsstelle, daß jeder Schlüssel in ihrem Zertifikatsverzeichnis nur einmal vorhanden ist. Bei der Erzeugung einer digitalen Signatur wird das relevante Signaturschlüssel-Zertifikat automatisch in die Signatur einbezogen, so daß selbst bei einem (theoretisch nicht völlig auszuschließenden) gleichen Schlüssel in einem anderen Zertifikatsverzeichnis bei mit gleichen Schlüssel erzeugten digitalen Signaturen die Urheber eindeutig zu unterscheiden wären.

Die Bindung des Signaturschlüssels an den Inhaber erfolgt durch Besitz (z.B. Chipkarte) und Wissen (PIN). Ein Mißbrauch des privaten Signaturschlüssels durch Unbefugte ist damit ausgeschlossen, soweit der Nutzer dafür sorgt, daß Karte und PIN Unbefugten nicht zugänglich sind.

Zusätzliche Sicherheit bringt die Nutzung biometrischer Merkmale. So können z.B. Fingerstrukturen erfaßt und auf der Chipkarte mit dem privaten Signaturschlüssel gespeichert werden. Der Signaturschlüssel wird erst nach Identifikation des rechtmäßigen Nutzers (Erfassung der Fingerstruktur über den Chipkartenleser) freigegeben. Durch mehrfache Identifikation – das heißt durch Besitz (Karte), Wissen (PIN) und Nutzung biometrischer Merkmale – kann ein Mißbrauch des privaten Signaturschlüssels praktisch vollständig ausgeschlossen werden. Als biometrisches Merkmal kann u.a. auch die eigenhändige Unterschrift (automatische Erfassung von Form, Dynamik, Druckverhalten) benutzt werden.

Im Handbuch des BSI zur digitalen Signatur werden auf der Basis modellhafter Lösungsvorschläge nach Auflistung der spezifischen Bedrohungen für die skizzierten Lösungsvorschläge Sicherheitsmaßnahmen vorgeschlagen, die gegen die genannten Bedrohungen wirken und die Anforderungen des Gesetzes und der Verordnung und Empfehlungen des Maßnahmenkatalogs erfüllen.

Es werden die Maßnahmen aufgeführt, die bei Entwicklung, Prüfung und Einsatz von technischen Komponenten nach SigG und SigV berücksichtigt werden sollen. Das betrifft die Bereiche:

- Kryptoalgorithmen,
- Schlüsselerzeugung,
- Zertifikatserstellung,
- Personalisierung der Signaturkomponenten,
- Verzeichnisdienste,
- Zeitstempeldienste,
- Anwenderinfrastruktur und
- Signaturkomponenten.

Die Vertrauenswürdigkeit des Gesamtsystems einer Zertifizierungsstelle in einem geprüften und bestätigten Sicherheitskonzept berücksichtigt die (bekannten) technischen, materiellen, personellen und organisatorischen Aspekte. Dabei ist insbesondere der Nachweis der Vertrauenswürdigkeit der relevanten technischen Komponenten zu erbringen. Dies betrifft die technischen Komponenten:

- Erzeugung und Speicherung von Signaturschlüsseln
- Erzeugung und Prüfung digitaler Signaturen
- Darstellung der zu signierenden Daten
- Nachprüfen von Zertifikaten
- Erzeugung und Vergabe von Zeitstempeln.

Ermöglicht das Signaturgesetz noch eine hinreichende Prüfung nach dem Stand der Technik (§14(4)) mit einer Bestätigung durch eine durch die Regulierungsbehörde anerkannten Stelle, so sind die Forderungen zur Komponentenprüfung in §17 der Signaturverordnung fest definiert. Als wesentliche Grundlage zur Komponentenprüfung werden die harmonisierten europäischen Sicherheitskriterien „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik – ITSEC“ in Verbindung mit der zugehörigen „Evaluationsmethodologie – ITSEM“ festgelegt [ITSE91], [ITSE94].

5. Nationale Struktur der Zertifizierungsinstanzen

Das zugrundeliegende nationale Schema wird gebildet durch eine 3-stufige Struktur aus Steuerinstanz (PCA: repräsentiert durch eine staatliche Institution: die sogenannte zuständige Behörde (wahrgenommen durch die Regulierungsbehörde für Telekommunikation und Post)), den sogenannten privaten Zertifizierungsstellen (CA) und der Anwenderebene und zielt somit auf eine praxisorientierte Kooperation zwischen Staat und Privatwirtschaft. Von Bedeutung ist dabei, daß das installierte Gesamtschema ein angemessenes und durchgehendes Sicherheitsniveau besitzt, widergespiegelt in allen Teilaspekten: seien es die Anforderungen an die Infrastruktur (z.B. die einzusetzende Technik, Organisation, Personal, Abläufe) oder seien es die Anforderungen an die zugrundeliegende Prüf- und Bestätigungsinfrastruktur. Dies ist insbesondere von Bedeutung, da im deutschen Ansatz keine Abstufung bezüglich des Sicherheitsniveaus vorgesehen ist.

6. Anwendungen und Nutzen
– z.B. digitaler Ausweis

Auf der Basis der Signaturschlüssel ist auch weltweit eine sichere Authentisierung beim Zugriff auf Rechner und Daten möglich. Signaturschlüssel-Zertifikate können für „digitale Ausweise“ eingesetzt werden, indem automatisch übermittelte Zufallswerte damit signiert und die Signatur beim Empfänger automatisch überprüft wird. Der Zugriff auf Daten – etwa in der Unternehmensdatenbank vom Telearbeitsplatz oder vom Hotelzimmer aus – kann davon abhängig gemacht werden, daß die betreffende Person sich entsprechend ausweist und autorisiert ist.

Auch die Annahme elektronischer Post kann künftig davon abhängig gemacht werden, daß der Absender sich durch digitale Signatur ausweist. Die Annahme kann absenderabhängig automatisch verweigert oder auf bestimmte Absender beschränkt werden. Die automatische Offenbarung der Urheberschaft elektronischer Post ermöglicht jeder natürlichen und juristischen Person einen wirksamen Selbstschutz vor unerwünschten Sendungen, z.B. mit strafbarem Inhalt oder dem Ziel der Überflutung des Datenspeichers. Damit und durch weltweit sichere Identifikation/Authentisierung kann auch partiell ein praktischer Jugendschutz beim Austausch digitaler Daten erreicht werden, z.B. durch Zugangsbeschränkung bei

bestimmten Informationsdienstleistungen oder Datenzugängen auf Erwachsene und Beschränkung der Annahme oder Weiterleitung elektronischer Post auf signierte Sendungen (so daß jederzeit der Urheber feststellbar ist).

7. Nationaler und internationaler Ausblick

Deutschland hat mit dem Signaturgesetz zwar international eine Vorreiterrolle übernommen, allerdings haben in der Zwischenzeit andere Staaten vergleichbare Entwürfe auf den Weg gebracht bzw. befinden sich in der abschließenden Diskussion (z.B. Italien, Dänemark, Belgien, Schweden, Niederlande, UK u.a.) [DDBDS97], [TTRG97].

In den USA ist die Kompetenz zur Regulierung über die digitalen Signaturverfahren den Einzelstaaten zugewiesen. Da wenig Einigkeit darüber besteht, welcher Regulierungsansatz zu favorisieren ist, bestehen mittlerweile 39 unterschiedliche, entweder bereits erlassene oder in der Planung befindliche, Gesetze zur digitalen Signatur. Der am 1. Mai 1995 in Kraft getretene Utah Digital Signature Act ist das Weltweit erste Gesetz zur digitalen Signatur. Es wird konkretisiert durch die Utah Digital Signature Adminintrative Rules, die von der Division of Corporations and Commercial Code des Department of Commerce erlassen wurden und seit dem 1. November 1997 in Kraft sind. [DuD 22 (1998)]

Deshalb kann man digitale Signaturen nach dem Signaturgesetz weltweit vorläufig nur anwenden, soweit auch die Kommunikationspartner über Zertifikate deutscher Zertifizierungsstellen verfügen. Auch wenn deutsche Zertifizierungsstellen im Ausland Annahmestellen für Zertifikatsanträge einrichten, dürfte dies nur in Einzelfällen weiterhelfen.

Um hier Abhilfe zu schaffen, hat die EU-Kommission einen ersten Entwurf einer EU-Rahmenrichtlinie zur digitalen Signatur dem EU-Rat vorgelegt. Danach sollen bis zum Jahre 2001 alle EU-Staaten harmonisierte, nationale Regelungen zur digitalen Signatur erlassen [ESTEC98]. Daneben gibt es Bestrebungen, zu einer weltweiten Anerkennung digitaler Signaturen zu gelangen (z.B. über die Welthandelskonferenz (UNCITRAL) [UNML97]).

Das Signaturgesetz sieht die Anerkennung ausländischer Zertifikate und digitaler Signaturen durch über- oder zwischenstaatliche Vereinbarungen ausdrücklich vor. Voraussetzung ist, daß diese eine vergleichbare Sicherheit aufweisen.

Weitere BSI-Informationen

Internet – Adresse:

http://www.bsi.bund.de

BSI-Projektbüro für digitale Signatur

http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/index.htm

Ansprechpartner für:

Anwenderberatung, Sicherheitskonzept: Fr. Rohde
Tel.: 0228/9582-285

Technische Komponenten: Hr. Keus / Hr. Dr. Schöller
Tel.: 0228/9582-141 / -115

Kryptographie: Hr. Dr. Liebetrau
Tel.: 0228/9582-646

Literatur:

[IUKD97] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IUKDG), Bundesgesetzblatt 1869, Teil1 G5702 (1997) 1869-1880.

[SigV97] Verordnung zur digitalen Signatur (Signaturverordnung – SigV), Stand 8. Oktober 1997.

[BSI97] Handbuch des BSI zur digitalen Signatur (Angaben des BSI zum Maßnahmenkatalog gemäß SigV §§ 12(2) und 16(6)), Ausgabe Version 1.0 vom 18.11.1997,

http://www.bsi.bund.de

[ITSE91] Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Kommission der Europäischen Gemeinschaft, EGKS-EWG-EAG (1991) ISBN 92-826-3003-x.

[ITSE94] Information Technology Security Evaluation Manual (ITSEM), Kommission der Europäischen Gemeinschaft, EGSG-EEG-EAEG (1993) ISBN 92-826-7087-2.

[DDBDS97] Danish Draft Bill on Digital Signature etc., Ministry of Research and Information Technology, IT-Policy Office, November 14, 1996

[ITRG97] Regolamento concemento „Atti, Documenti e Contratti in Forma Electronica“,

http://www.notariato.it/forum/

[ESTEC98] Ensuring Security and Trust in Electronic Communication, Draft communication from the Commission to the European Parlament, the Council, the Economic and Social Committee and the Committee of the Regions, EG DG XIII; Telecommunications, Information Market and Exploitation of Research, Brussels

[UNML97] UNCITRAL: Model Law on Electronic Commerce with Guide to Enactment, United Nations, V.97-22269 May 1997-5,100.

[DuD 22 (1998)] Regelungsansätze und –struktur der US-amerikanischen Signaturgesetzgebung von Anja Miedbrodt**,** DuD Datenschutz und Datensicherheit 22 (1998).