Dr. André Helmke
Assessor jur.
Dipl.-Verwaltungswirt (FH)
Rampenstr. 2
27568 Bremerhaven
Tel: 0471 48139589
www.andre-helmke.de
www.justitia21.de

Bremerhaven, 13. Oktober 2011

Zugangssicherung und Digitale Signatur mit Smartcards

Skriptum

1999 - 2011

Inhaltsverzeichnis

Zugangssicherung und Digitale Signatur mit Smartcards

I. ***Einführung in das Thema***

Das Internet gewinnt immer mehr Bedeutung für die Informationsgesellschaft. Offene Systeme sollen die Kommunikation zwischen Rechnern unterschiedlicher Hersteller, offene Netze eine Kommunikation zwischen Rechnern und Benutzern und Benutzern untereinander weltweit ermöglichen[1].

Dies hat auch die öffentliche Verwaltung erkannt, wobei hierzu alle Stellen gehören, die öffentliche Aufgaben wahrnehmen (Städte, Gemeinden, Gerichte, Staatsanwaltschaften usw.). Einschlägige Umfragen haben gezeigt, dass Bürgerinnen und Bürger ebenso wie Wirtschaft und Institutionen ein großes Interesse daran haben, ihre Kontakte zu den unterschiedlichsten Verwaltungen künftig schneller, einfacher und günstiger abwickeln zu können (Schaffung sogenannter Virtueller Rathäuser bzw. Virtueller Kommunen). Eine wesentliche Forderung ist die Einbeziehung von elektronischen Kommunikationstechniken in das Verwaltungshandeln.

Dabei lautet die Maxime: Wie bringe ich auf schnellstem Wege die richtige Information zum richtigen Zeitpunkt an den richtigen Ort zur berechtigten Person?[2]

Demzufolge ist jedoch auch die Frage zu beantworten: Wie ist zu verhindern, dass eine nicht berechtigte Person auf diese Informationen zugreifen kann? Das Problem dabei ist, dass die Zahl der Personen, die weltweite Netze nutzt und Informationen austauscht, Tag für Tag zunimmt und weit in die Millionen reicht.

1Kiefer, HMD 190/1996, 48, 48
2Kiefer, HMD 190/1996, 48, 48

Die Beantwortung dieser Frage ist von aktueller Bedeutung, da zukünftig auch Rechtsanwälte und Notare ihre Schriftsätze elektronisch bei Gericht einreichen werden können (sogenanntes Electronic Government oder kurz: E-Government). Das Bundeskabinett hat kürzlich (siehe FAZ vom 04.08.2004, Seite 19) einen Entwurf eines Justizkommunikationsgesetzes beschlossen. Mit diesem Gesetzesentwurf werden dem Zivilprozess und den Fachgerichtsbarkeiten der Weg für eine elektronische Aktenbearbeitung eröffnet. So können mehrere Bearbeiter gleichzeitig an einer Akte arbeiten. Zudem sind elektronisch übersandte Dokumente viel schneller beim Empfänger als Briefe.

Die Verfahrensbeteiligten (Richter, Rechtsanwälte, Notare, Bürger) sollen künftig die Möglichkeit haben, elektronische Kommunikationsformen gleichberechtigt neben der - herkömmlichen papiergebundenen - Schriftform oder der mündlichen Form rechtswirksam zu verwenden. Die bisherigen Formerfordernisse sollen auch bei der Nutzung eines elektronischen Übertragungswegs qualitativ unverändert bleiben. Um die Unterschiede des geltenden Rechts auf die elektronische Arbeit zu übertragen, differenziert der Entwurf zwischen einfacher, fortgeschrittener, qualifizierter oder einer elektronischen Signatur, die auf einem dauerhaft überprüfbaren Zertifikat beruht. Letztere wird derzeit nur von akkreditierten Zertifizierungsdienstleistern (sog. Trustcenter) angeboten.

Eine einfache elektronische Signatur, also z. B. der Namenszusatz, ist dann ausreichend, wenn das Gesetz bisher bereits keine besondere Form vorschreibt und keine Gewähr für die Identität des Signierenden oder die Authentizität des Inhalts

erforderlich ist. Fortgeschrittene elektronische Signaturen liegen nur dann vor, wenn eine Reihe von Mindestanforderungen erfüllt sind. Schon jetzt kann aber meines Erachtens gesagt werden, dass der Beweiswert einer einfach bzw. fortgeschritten signierten E-mail vor Gericht gering ist, wenn nicht weitere Indizien für die Authentizität vorgetragen werden.

Soweit gesetzliche Schriftform i. S. d. § 126 BGB vorgeschrieben ist, wird die qualifizierte elektronische Signatur vorgeschrieben. So führt § 126 Abs. 2 BGB n. F. nun aus, dass die schriftliche Form durch die elektronische Form ersetzt werden kann, wenn sich nicht aus dem Gesetz ein anderes ergibt. Aus dem letzten Halbsatz wird deutlich, dass die qualifizierte elektronische Signatur nicht ausnahmslos die schriftliche Form i. S. d. § 126 BGB ersetzt. Beispielsweise bleibt für § 623, letzter Halbsatz BGB (Kündigung und Auflösungsvertrag eines Arbeitsverhältnisses) oder für die Bürgschaft (§ 766 Satz 2 BGB) weiterhin das Schriftformerfordernis bestehen.

Die qualifizierte elektronische Signatur erfordert einen öffentlichen und einen persönlichen Signaturschlüssel, die von einer Zertifizierungsstelle ausgegeben werden. Der Inhaber dieser Schlüssel enthält eine Smartcard, welche beide Schlüssel enthält und mit einer persönlichen PIN nur durch den Inhaber berechtigt verwendet werden kann. Dadurch werden beim Signieren die Identität des Absenders und die Authentizität des Inhalts des Dokumentes sichergestellt. Möglich ist weiterhin eine Verschlüsselung des Dokumentes und damit eine Sicherung der Vertraulichkeit. Um ein Maximum an Authentizität zu garantieren, übernimmt der Staat die staatliche Aufsicht und Kontrollfunktion

ein. Oberste Aufsichtsbehörde gem. § 3 Signaturgesetz (SigG) ist die Regulierungsbehörde für Post- und Telekommunikation (RegTP). Soweit die technisches Voraussetzungen erfüllt sind, regelt schon jetzt § 126 a Abs. 1 BGB, wie eine elektronische Form zustande kommt. Soll danach die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur versehen. Gemäß § 126 a Abs. 2 BGB müssen bei einem Vertrag die Parteien jeweils ein glauchlautendes Dokument in der in Absatz 1 bezeichneten Weise elektronisch signieren.

Das bereits vor wenigen Jahren in Kraft getretene Signaturgesetz regelt lediglich die Integrität der elektronischen Dokumente und die Authentizität der Partner, nicht aber die Vertraulichkeit. Anders gesagt: Wie wird sicher gestellt, dass Herr Rechtsanwalt Meier und Herr Richter Müller auch wirklich diejenigen Personen sind, für welche sie sich ausgeben (Authentizität). Und: wie kann bewiesen werden, dass die ausgetauschten Dokumente auch wirklich von diesen Personen stammen und dass die Inhalte der Dokumente unverfälscht sind (Integrität).

Nicht selten liest oder sieht man Berichte, dass Hacker in Computer bei der NASA oder im Pentagon eingedrungen sind[3]. Es gilt also möglichst einfache, vom Nutzer aktzeptierbare und sichere aber auch bezahlbare, administrierbare Mechanismen zu entwickeln, mit denen die Nutzung von Datennetzen und Rechnern und im Nachgang der Zugriff auf Daten und Programme gesteuert

3Siehe nur Schmidt, FAZ vom 11.02.2002, Seite 24; ähnlich auch NZ vom 30.07.2004, Seite 1

werden kann[4].

Zu den wichtigsten Maßnahmen für die Datensicherheit gehört daher die zuverlässige Kontrolle des Zutritts zu Gebäuden und Räumen, des Zugangs zu Systemen, Rechnern oder PCs und die sichere Kontrolle des Zugriffs auf Daten und Programme[5]. Entscheidend ist dabei die einwandfreie Identifizierung der Berechtigten. Bei einem persönlichen oder telefonischen Gespräch kennen sich die Partner oder identifizieren sich an vielerei Merkmalen, z. B. über die Stimme oder umfangreiche gemeinsame Kenntnisse des Gesprächsthemas. Erst nach sicherer Identifikation werden vertrauliche Informationen ausgetauscht. Technischen Kommunikationseinrichtungen fehlt jedoch (noch!) die Fähigkeit, Menschen an ihren besonderen Attributen, Eigenschaften oder sonstigen individuellen Kennzeichen zu identifizieren, weil Menschen kein technischen "Interface" besitzen, das elektronisch abgefragt werden kann[6]. Damit sich der Mensch gegenüber einem technischen Gerät oder gegenüber einem anderen Menschen, mit dem er über das Internet kommuniziert, identifizieren kann, wird heute die sogenannte Smartcard favorisiert[7]. Herz und Hirn der Smartcard ist ein winziger vollwertiger Microcontroller. Im Chip sind ein Prozessor, verschiedene Speicher und ein Betriebssystem untergebracht. Dort werden Pins und andere sicherheitsrelevante Informationen wie kryptographische Schlüssel und die zugehörigen Verschlüsselungsalgorithmen sicher verwahrt. Her-

4Kiefer, HMD 190/1996, 48, 48
5Kruse/Peuckert, DuD 1995, 142, 146
6Kruse/Peuckert, DuD 1995, 142, 146 f.
7smart: geschickt; gerissen; sauber; elegant; fein; forsch; patent; u. ä.

kömmliche Sicherungsmittel wie Ausweise, Passwörter und Berechtigungsscheine reichen nicht mehr aus. Der Fortschritt der Technik wird nicht nur von den Ausweisherstellern, sondern auch von Ausweisfälschern genutzt.

Die für die Zugangskontrolle und Digitale Signatur erforderliche Technik ist bei den Gerichten und Anwälten weitgehend vorhanden. Anwälte müssen sich neben einem Computer lediglich eine solche Smartcard (= Signaturkarte) nebst Kartenlesegerät und die dazugehörige Software anschaffen.

Die Justiz wird einen elektronischen Gerichtsbriefkasten einrichten, an den Anwälte elektronisch signierte Schriftsätze werden schicken können. Vom Gericht wird der Anwalt sodann automatisch eine Eingangsbestätigung erhalten. Damit sei dieser Kommunikationsweg genauso sicher wie ein Einschreiben.

Aber wodurch wird diese Sicherheit gewährleistet oder anders ausgedrückt: Ist dieser Kommunikationsweg wirklich so sicher? Wie wird garaniert, dass die per E-mail auf diese Art und Weise bei Gericht eingereichten Schriftsätze wirklich von den Prozessbevollmächtigten mit dem bei Gericht angekommenen Inhalt abgesendet worden sind?

II. ***Rechtliche Rahmenbedingungen durch das geplante Justizkommunikationsgesetz (JKomG-BReg)***

Bereits mit dem Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr (FormVorAnpG) vom 13. Juli 2001 (BGBl I S. 1542) sowie mit dem Gesetz zur Reform des Verfahrens bei Zu-

stellungen (ZustRG) vom 25. Juni 2001 (BGBl I S. 1206) wurden erste Schritte zu einer Öffnung der Justiz für einen elektronischen Rechtsverkehr unternommen. Diese Gesetze enthalten die rechtlichen Grundlagen für eine Einreichung elektronischer Schriftsätze bei Gericht sowie für elektronische Zustellungen vom Gericht an einen festgelegten Personenkreis[8].

Mit dem Regierungsentwurf eines Justizkommunikationsgesetzes (JKomG-BReg) sollen nun die rechtlichen Grundlagen für die Einreichung elektronischer Schriftsätze bei Gericht sowie elektronische Zustellungen an einen bestimmten Personenkreis geschaffen. Der Gesetzentwurf regelt die rechtlichen Rahmenbedingungen, unter denen Anwältinnen und Anwälte aber auch Notarinnen und Notare ihre Schriftsätze statt in Papierform künftig elektronisch bei Gericht einreichen können. Auch für die Justiz ist der elektronische Rechtsverkehr attraktiv, weil er Abläufe vereinfacht und beschleunigt.

Um eine umfassende elektronische Aktenbearbeitung innerhalb des Gerichts zu ermöglichen, besteht für die auf dem Medium "Papier" basierenden gerichtlichen Verfahren weiterer Gesetzgebungsbedarf in den einzelnen Verfahrensordnungen.

Durch das Gesetz wird der Zivil-, der Arbeitsgerichts-, der Verwaltungs-, Finanz- und Sozialgerichtsprozess und das Ordnungswidrigkeitenverfahren umfassend für den elektronischen Rechtsverkehr geöffnet. Im Bereich des Strafverfahrens wird die Möglichkeit eröffnet, elektronisch zu kommunizieren. Das herkömmliche Prozessrecht geht von der Papierform aus und muss deshalb so umgestaltet werden, dass es für die neuen Techniken

8JKomG-BReg, Seite 53

geöffnet wird. Der Entwurf enthält Regelungen, die Anforderungen an elektronische Dokumente festschreiben, denn auch bei elektronischen Dokumenten muss sichergestellt sein, dass das Dokument authentisch ist, also tatsächlich von seinem Verfasser stammt und auch nicht verändert worden ist. Deshalb sieht der Gesetzentwurf vor, dass elektronisch abgefasste Urteile mit einer qualifizierten elektronischen Signatur zu versehen sind. Sogenannte bestimmende Schriftsätze, wie z. B. Klageschriften, müssen grundsätzlich ebenfalls qualifiziert elektronisch signiert sein. Weiter enthält der Entwurf Regelungen über die elektronische Akteneinsicht, über den Beweiswert elektronischer Dokumente und über den Medientransfer, also über die Umwandlung von Papierdokumenten in elektronische Dokumente.

Der Bund hat bereits durch die Verordnung über den elektronischen Rechtsverkehr beim Bundesgerichtshof (ERVVOBGH) vom 26. November 2001 (BGBl I S. 3225) von der Verordnungsermächtigung des § 130 a Abs. 2 ZPO Gebrauch gemacht und dadurch die rechtlichen Grundlagen für den elektronischen Zugang zu den Zivilsenaten des Bundesgerichtshofs geschaffen. Seit dem 30. November 2001 können elektronische Dokumente wirksam bei zwei Bundesgerichten, dem Bundesgerichtshof und dem Bundespatentgericht, bereits jetzt Dokumente elektronisch eingereicht werden. Ende dieses Jahres soll dies auch beim Bundesverwaltungsgericht und beim Bundesfinanzhof möglich sein.

Bund und Länder haben zudem gemeinsam detaillierte organisatorisch-technische Leitlinien (OTLeit) entwickelt, die technische Standards und Formate für den elektronischen Rechtsverkehr mit den Gerichten festlegen. Diese sollen die

Grundlage für die Rechtsverordnungen der Länder werden, mit denen die elektronische Kommunikation eingeführt wird[9].
Im folgenden sollen ein paar geplante konkrete Gesetzesänderungen bzw. -ergänzungen vorgestellt werden:

1.**§ 371 a ZPO-E (Beweiskraft elektronischer Dokumente)**

a)Geplanter Gesetzestext

Gemäß Artikel 1 Nr. 29 soll nach § 371 folgender § 371 a eingefügt werden:

"§ 371 a
Beweiskraft elektronischer Dokumente

(1) Auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, das die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.

(2) Auf elektronische Dokumente, die von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des

9JKomG-BReg, Seite 54

ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind (öffentliche elektronische Dokumente), finden die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Ist das Dokument mit einer qualifizierten elektronischen Signatur versehen, gilt § 437 entsprechend."

b)Amtliche Begründung

Nach Inkrafttreten des Justizkommunikationsgesetz wird zukünftig verstärkt mit elektronischen Beweismitteln zu rechnen sein. Das elektronische Dokument unterfällt grundsätzlich dem Beweis durch Augenschein. Die Beweiskraft eines öffentlichen und eines privaten elektronischen Dokuments (§ 371 a Abs. 1 und 2 ZPO-E) richtet sich, sofern es mit einer qualifizierten elektronischen Signatur versehen ist, jeweils nach den Vorschriften über die Beweiskraft der jeweiligen Urkunde.
§ 371 a Abs. 1 ZPO-E regelt die Beweiswirkung von privaten elektronischen Dokumenten, die mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen sind. Sie begründen, sofern sie als echt anzuerkennen sind, vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen vom Signaturschlüsselinhaber abgegeben worden sind. Die Echtheit der Signatur hat der Beweisführer zu beweisen. Hierbei hilft ihm, sofern er sich auf eine ihm zugegangene Erklärung des Signatur-schlüsselinhabers beruft, ein Anscheinsbeweis (Absatz 1 Satz 2). Dieser aus der bisherigen Regelung des § 292 a ZPO entnommene Rechtsgedanke gilt nunmehr für alle in elektronischer Form

vorliegenden Erklärungen, auch für Wissenserklärungen wie beispielsweise Quittungen[10].

Damit wird dem Empfänger einer in elektronischer Form (§ 126 a BGB) abgegebenen Erklärung durch eine gesetzliche Regelung der von der Rechtsprechung entwickelten Grundsätze zum Beweis des ersten Anscheins die Beweisführung erleichtert. Hierdurch wird seine Rechtsstellung im Prozess wesentlich gestärkt und im Hinblick darauf das Vertrauen in die Rechtssicherheit und die Verkehrsfähigkeit der elektronischen Form in besonderem Maße gewährleistet. Der Nachweis der Echtheit der in dieser Form abgegebenen Erklärung wird danach grundsätzlich schon durch die Prüfung nach dem Signaturgesetz erbracht, die die Signierung mit dem auf der Signaturchipkarte gespeicherten geheimen Schlüssel des Inhabers und dessen Identität bestätigt. Der Inhaber des Schlüssels kann diesen Nachweis nur erschüttern, wenn er schlüssig Tatsachen vorträgt und beweist, die einen abweichenden Geschehensablauf ernsthaft als möglich erscheinen lassen. Damit wird ein weitergehender Schutz des Erklärungsempfängers erreicht, als es die Vorschriften der Zivilprozessordnung über den Beweis durch Schrifturkunden vermögen, da nach diesen eine entsprechende Beweiserleichterung nicht eintritt, sondern der Erklärungsempfänger den vollen Beweis der Echtheit einer von dem Beweisgegner nicht anerkannten Namensunterschrift erbringen muss (§ 439 Abs. 1 und 2, § 440 Abs. 1 ZPO)[11].

Die neue Vorschrift des § 371 a Abs. 2 Satz 1 ZPO-E stellt den Beweiswert öffentlicher elektronischer Dokumente (§§ 3 a, 33, 37

10JKomG-BReg, Seite 79
11JKomG-BReg, Seite 79

VwVfG) dem Beweiswert entsprechender öffentlicher Urkunden gleich, indem sie für diese Dokumente die Vorschriften über die Beweiskraft öffentlicher Urkunden für anwendbar erklärt. Die Vorschrift bekräftigt damit zugleich die gesetzgeberische Leitentscheidung, dass elektronische Dokumente dem Beweis durch Augenschein unterfallen.

Durch diese Verweisung sind sowohl die allgemeinen Beweiskraftregeln in §§ 415, 417, 418 ZPO als auch die speziellen Vorschriften über die Beweiskraft des gerichtlichen Protokolls (§ 165 ZPO) und des Urteilstatbestandes (§ 314 ZPO) erfasst. Protokolle und Urteile, die in elektronischer Form vorliegen, genießen also dieselben beweisrechtlichen Wirkungen wie ihre Papierentsprechungen[12].

Die beweisrechtliche Gleichstellung des elektronischen Dokuments mit der Papierurkunde ist notwendige Voraussetzung für einen medienbruchfreien elektronischen Rechtsverkehr. Sie gewinnt ihre Bedeutung insbesondere in den öffentlich-rechtlichen Verfahrensordnungen.

Der verfahrensbeteiligten Behörde ist es künftig möglich, in ihren Dateien gespeicherte Dokumente, insbesondere Verwaltungsakte, ohne die Gefahr eines Rechtsverlustes in elektronischer Form an das Gericht zu übermitteln[13].

Die Gleichstellung kann verantwortet werden, weil die in der nach § 130 b ZPO-E (Gerichtliches elektronisches Dokument) oder §§ 3 a, 33 VwVfG vorgeschriebenen Form vorhandenen öffentlichen elektronischen Dokumente gegen Veränderung in zumindest äqui-

12JKomG-BReg, Seite 79 f.
13JKomG-BReg, Seite 80

valenter Weise geschützt sind wie eine Urkunde.
In Signaturschlüssel-Zertifikaten oder in Attribut-Zertifikaten können alle Funktionen, Zuständigkeiten, Rechte usw. von Behördenmitarbeitern ausgewiesen werden. Auch Dienstsiegel können elektronisch abgebildet werden. Absatz 2 Satz 2 gewährt aus diesen Gründen öffentlichen elektronischen Dokumenten, die qualifiziert signiert worden sind, die Vermutung der Echtheit durch eine entsprechende Anwendung der für die öffentliche Urkunde geltende Beweisregel des § 437 ZPO. Durch die verwendeten Zertifikate ist es für das Gericht im Rahmen der Signaturprüfung möglich festzustellen, wer das öffentliche elektronische Dokument mit welchem Inhalt erstellt hat[14].

2.**Mahnbescheide in elektronischer Form**

Eine Ergänzung im Regierungsentwurf stellt klar, dass der Mahnbescheid in elektronischer Form ergehen kann, wenn das Dokument mit einer einfachen elektronischen Signatur versehen wird. Wegen der Entbehrlichkeit der handschriftlichen Unterzeichnung gilt § 130 b ZPO-E für den Mahnbescheid nicht. Diese geringere Formenstrenge wird für den elektronischen Mahnbescheid durch die Zulassung der einfachen Signatur nachvollzogen.

3.**§ 39 a BeurkG (Einfache elektronische Zeugnisse)**

Gemäß Artikel 8 Nr. 2 soll nach § 39 folgender § 39 a eingefügt werden:

14JKomG-BReg, Seite 80

"§ 39 a
Einfache elektronische Zeugnisse

Beglaubigungen und sonstige Zeugnisse im Sinne des § 39 können elektronisch errichtet werden. Das hierzu erstellte Dokument muss mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen werden. Diese soll auf einem Zertifikat beruhen, das auf Dauer prüfbar ist. Mit dem Zeugnis muss eine Bestätigung der Notareigenschaft durch die zuständige Stelle verbunden werden. Das Zeugnis soll Ort und Tag der Ausstellung angeben."

Demnach erhalten auch Notare/Innen die Möglichkeit, im elektronischen Bereich zu beglaubigen. Der im Beurkundungsgesetz verwendete Begriff "auf Dauer prüfbar" ist funktionell zu verstehen.

4.**Zwangsvollstreckung**

Im Bereich der Zwangsvollstreckung kann derzeit auf die Erteilung einer vollstreckbaren Ausfertigung in der herkömmlichen Papierform nicht verzichtet werden, soweit die Vollstreckung/-Beitreibung nicht wie im Bereich des Bußgeldverfahrens durch den Staat als Gläubiger betrieben und die dabei beigetriebenen Beträge in einem Vollstreckungsheft vermerkt werden. Der zum Schutz des Schuldners unerlässliche Grundsatz der Einmaligkeit der vollstreckbaren Ausfertigung (§§ 733, 757 ZPO) steht der

Verwendung elektronischer vollstreckbarer Ausfertigungen noch entgegen, da diese unbeschränkt vervielfältigt werden können. Auch der Umstand, dass Zahlungen des Schuldners auf der vollstreckbaren Ausfertigung zu vermerken sind und die Ausfertigung dem Schuldner nach vollständiger Erfüllung auszuhändigen ist, steht der Verwendung elektronischer Ausfertigungen vorläufig entgegen. Erst nach Einführung eines bundesweiten elektronischen Vollstreckungsregisters und einer grundlegenden Umgestaltung des Vollsteckungsverfahrens kann auf die Erteilung herkömmlicher vollstreckbarer Ausfertigungen verzichtet werden[15].

5. **Strafverfahren**

Im Strafverfahren soll derzeit keine vollständig elektronisch geführte Akte eingeführt werden[16]. Zum einen können Niederschriften über die Vernehmung von Beschuldigten und Zeugen als nach Umfang und Bedeutung wesentliche Teile der Ermittlungsakte nicht ohne erhebliche Beeinträchtigung ihres Beweiswerts durch elektronische Dokumente ersetzt werden. Des weiteren würde derzeit die verbindliche Festlegung etwa des Beschuldigten, des Verteidigers oder des Nebenklägers auf papierlose Kommunikation mit den Strafverfolgungsorganen wesentliche, mit dem Verfassungsprinzip des rechtlichen Gehörs kaum vereinbare Zugangsschranken errichten. Gerade am Strafverfahren sind vielfach Personen beteiligt, die aufgrund ihrer sozialen Herkunft auch zukünftig nicht über die erforderliche technische Ausstattung

15 JKomG-BReg, Seite 58
16 JKomG-BReg, Seite 58

oder die notwendigen Kenntnisse verfügen werden[17].
Dagegen kann bereits heute das Serviceangebot der Justiz durch die Einfügung des § 41 a StPO-E verbessert werden. Während der Ausgang von Zustellungen und formfreien Mitteilungen von Schriftstücken auf elektronischen Wege seit 1.7.2002 nach dem über § 37 Abs. 1 S. 1 StPO anwendbaren § 174 Abs. 3 ZPO möglich ist, regelt § 41 a StPO-E den Eingang elektronischer Dokumente bei Gericht und Staatsanwaltschaft. Dem Verfahrensbeteiligten bleibt freigestellt, ob er Dokumente auf elektronischem Wege übermittelt; die Strafverfolgungsorgane eröffnen mit dem elektronischen Rechtsverkehr einen zusätzlichen Kommunikationsweg.

III. ***Eingrenzung des Untersuchungsthemas***

1. **Was bedeutet Zugang?**

Nach Nr. 1 der Anlage zu § 9 Satz 1 BDSG[18] bedeutet Zugangskontrolle, Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.
Demgegenüber umschreibt Jäger[19] die Zugangskontrolle extensiver: Die befugten Personen müssen individuell zweifelsfrei identifiziert werden - Wer meldet sich an? Wer will in welchen Rechner und in welches Netz hinein? Welche Befugnisse besitzt er?
Dem ist zuzustimmen. Die Zugangskontrolle darf nicht hinter der Eingangspforte zum (lokalen) Netzwerk enden. Den Begriff

17 JKomG-BReg, Seite 59
18 Sartorius I, Nr. 245
19 Jäger, COMPUTERWOCHE Nr. 42 vom 16.10.1998

"Zugang" zu einem Rechner oder zu einem Netzwerk verwende ich daher für den Prozess, der den physischen Zugang zum Rechner und/oder die Nutzung des Betriebssystems und/oder den Zugriff auf Programme und Daten umfasst. Mit dieser Definition umfasst Zugangssicherung sämtliche Schutzvorkehrungen gemäß der Anlage zu § 9 Satz 1 BDSG[20].

2. Was bedeutet Sicherheit?

Bevor man sich mit der Zugangssicherung und der Digitalen Signatur befasst, macht es sicher Sinn, sich der Bedeutung des Wortes "Sicherheit" zu vergewissern. Die Sicherheit ist für uns Menschen ein wichtiger Faktor in unserem Leben: Wir wollen uns gegen Risiken absichern und gegen Schäden versichern, sichern unseren Besitzstand und benötigen von Zeit zu Zeit "sichere" Informationen, um wichtige Entscheidungen treffen zu können[21]. Dort, wo sicher kommuniziert werden soll, wird Verschlüsselung als probates Mittel angesehen. Leider können sich dieser Techniken auch Kriminelle bedienen.

3. Angreifer und Angriffsarten

Bei jeder Überlegung bezüglich der verschiedensten Sicherheits-aspekte ist es nötig abzuschätzen, gegen wen man sich schützen möchte. Dies ist die Grundlage für die Überlegung, wieviel Aufwand in die entsprechenden Schutzaktivitäten investiert wird.

20Ähnlich auch die ISO 7498-2 Sicherheits-Standards, in: Stollenmayer, HMD 190/1996, 61 ff.
21Siehe nur Kersten, HMD 190/1996, 5, 5

Grundlegend gibt es fünf Gruppen von Angreifern, die mit unterschiedlichem Wissen und unterschiedlichen Voraussetzungen mehr oder minder bewusst versuchen, die Sicherheitsvorkehrungen einer Organisation zu untergraben[22]:

-verärgerte ehemalige Mitarbeiter,
-unehrliche Mitarbeiter,
-Mitbewerber,
-Hacker,
-Mitarbeiter mit schlechter Schulung.

Ein sicheres Netz muss daher fünf Typen von Attacken abwehren können[23]:

-Ausspähung:
Schutz gegen das Mitlesen von Informationen. Dies schließt auch Passwörter und PINs ein.
-Verlust der Integrität:
Schutz gegen die Manipulation von Inhalten (beispielsweise in einem Vertrag die Änderung einer Summe von 10.000 EUR in 100.000 EUR oder umgekehrt).
-Unerlaubte Handlungen:
Darunter fällt eine Vielzahl denkbarer Aktivitäten. Dies reicht von der Vireneinschleusung über das Lahmlegen von Rechnern bis zur Blockade ganzer Netze.
-Identitätsfälschung:
Die Partner auf beiden Seiten der elektronischen Kommunikation müssen sich über die Identität des jeweils anderen absolut

22Vgl. ausführlicher dazu Reiser, 1998, S. 28 f.
23Jäger, COMPUTERWOCHE Nr. 42 vom 16.10.1998

sicher sein (mit wem rede ich?). Es darf also nicht möglich sein, Inhalte unter einem fremden Namen zu versenden.

-Ableugnung:

Dies ist der umbekehrte Fall - einer der (echten) Partner bestreitet nachträglich, dass und mit welchem (echten) Inhalt die Kommunikation stattgefunden hat. Auch dagegen wird ein Schutzmechanismus benötigt.

Alle Sicherheitsservices mit den verschiedenen Sicherheitsmechanismen und Sicherheitsobjekten zu beschreiben ist nicht Gegenstand dieser Ausarbeitung. Deshalb beschränke ich mich im nachfolgenden Text auf die klassischen Verfahren der Zugangssicherung und die mögliche Verbesserung insbesondere durch den Einsatz von kryptographischen Verfahren mit Smartcards.

IV. ***Klassische Sicherungskonzepte***

1. **Organisation**

Bei der Organisation von Sicherheitskonzepten geht es um allgemeine, aber wesentliche Fragen: Wer hat prinzipiell Zugang zu welchen Informationen und wer nicht? Dabei spielt die Auswahl des richtigen Personals eine entscheidende Rolle.

Es gibt darüber hinaus eine Gruppe von Menschen, die nicht die Absicht haben, der Organisation, in der sie arbeiten, zu schaden. Viele Sicherheitsvorfälle entstehen dadurch, dass ein interner Mitarbeiter etwas macht, wovon er nicht einmal ahnt, dass es gefährlich sein könnte. Es ist daher ausgesprochen

wichtig, dass Sicherheitsbewusstsein bei den eigenen Mitarbeitern durch entsprechende Schulungen zu heben, und sie mit einfachen Richtlinien[24] bzw. Weisungen[25] zu unterstützen. Eine allen Mitarbeitern bekannte Person sollte für informelle Anfragen zu diesem Thema zur Verfügung stehen.

2. **Passwörter**

Historisch gesehen sind Passwörter der am meisten genutzte Mechanismus für die Beglaubigung. Auch heute noch sind Passwörter ausreichend, wenn es um die Zugangssicherung zu herkömmlichen, kostenpflichtigen Inhalten im Internet geht[26]. Zwar sind sie einerseits kostengünstig, auf der anderen Seite soll das Passwort sicher sein. Das größte Sicherheitsrisiko für die Passwortintegrität entsteht bei der Übertragung in Datennetzwerken. Um die Sicherheit der Passwörter zu erhöhen, wurden einige Passwort-Managementfunktionen implementiert[27].

3. **Firewalls**

Ist ein Firmennetz am Internet angeschlossen, so kann im Prinzip von jedem Rechner des Internet auf dieses Firmennetz zugegriffen werden. Eine Lösung der Zugangssicherung ist eine "kontrollierte" Anschaltung eines Systems ans Internet. Firewalls

24Reiser, 1998, S. 29, 116 ff.
25Vgl. dazu Schäfer, 1997, S. 60 f.
26Siehe z. B. www.justitia21.de (ein juristisches Expertensystem für jedermann), wobei die Paßwörter auf dem Server verschlüsselt abgelegt werden.
27Näheres dazu vgl. Kiefer, HMD 190/1996, 48, 55 f.

schützen abgrenzbare Netzabschnitte gegen unbefugten Zugang und wirken wie Schutzmauern um eine Festung[28]. Hierfür sind firmeninterne Sicherheitsmaßnahmen nötig, mit dem Ziel, das interne System gegen Angriffe von außen zu schützen und trotzdem den Nutzern Zugang zu den benötigten Internet-Diensten zu geben[29]. Technisch realisiert wird dies durch eine Kontrollstelle, "Firewall" genannt, die zwischen das interne System und das Internet geschaltet wird. Ohne Firewall wäre das gesamte interne System für einen Angreifer von außen völlig transparent.

Der einfachste Firewall ist ein Adressfilter, der bestimmte IP-Adressen durchlässt und andere sperrt. Funktional mächtigere Firewalls blockieren ganze Dienste (zum Beispiel Telnet, Remote Login) oder führen bei den Diensten Prüfungen (zum Beispiel Formatanalyse, Vierenanalyse) durch.

Normalerweise ist die Gesamtfunktion eines Firewalls auf verschiedene Geräte (Router, Server, Hosts) verteilt, die jedes für sich zur geforderten Sicherheit beitragen. Das Herz dies Systems ist jedoch der sogenannte "Bastian Host", durch den der gesamte Verkehr nach außen und von außen geht[30]. Im Bastian Host sind die detaillierten Elemente der geforderten Sicherheit implementiert. Server für die verschiedenen Dienste (file transfer FTP, electronic mail, WWW-Zugang) übernehmen die dienstespezifischen Sicherheitsaufgaben.

Diese Technik erlaubt ferner eine "Netzwerk-zu-Netzwerk-Sicherheit" oder "Host-zu-Host-Sicherheit, je nachdem, wie sie

28Jäger, COMPUTERWOCHE Nr. 42 vom 16.10.1998; ausführlich dazu auch bei Reiser, 1998, S. 45 ff.
29Stollenmayer, HMD 190/1996, 61, 71
30Stollenmayer, HMD 190/1996, 61, 72

implementiert wird. Gebräuchlich ist, Verschlüsselung zwischen Firewalls über öffentliche Netzstrecken einzusetzen. Auf diese Weise kann ein sicherer Tunnel zwischen Intranets auch über öffentliche Netzwerke eingerichtet werden[31].

Die Grenzen der Firewalls liegen darin, dass sie keinen Schutz gegen Verlust von Integrität oder Vertraulichkeit bieten. Insbesondere können Firewalls nicht gegen Angriffe von innen schützen. Im wesentlichen sind sie eine zusätzliche Zugriffskontrolle, die eine Sicherheitsdomäne gegenüber dem Rest der Welt schützt. Insgesamt bieten Firewalls einen wertvollen zusätzlichen Schutz.

5. **Tempest**

Tempest ist ein englisches Kunstwort, das für "Temporary Emanation and Spurious Transmissions" steht und die elektromagnetische Abstrahlung von Geräten und Datenleitungen meint[32]. Was auf dem Monitor erscheint, kann auch aus größerer Entfernung mitgelesen werden - sogar durch normale Wände und Fenster hindurch. Die Abschirmung von Geräten und Gebäuden ist die teuerste Barriere gegen unerlaubtes Ausspähen des elektronischen Datenverkehrs. Man findet sie daher vor allem bei Computern für militärische Zwecke.

6. **Schrittweise Zugangssicherung**

31Näheres dazu bei Wise/Jäger, 1998, S. 6 f.
32Jäger, COMPUTERWOCHE Nr. 42 vom 16.10.1998

Des weiteren hat sich in der Vergangenheit folgende schrittweise Zugangssicherung bewährt:

a)Identifizierung der Nutzer durch Authentisierung

Der erste Schritt zur Durchführung einer "sicheren" Datenverarbeitung ist die zweifelsfreie Bestimmung der Identität des Benutzers, da nur so erreicht werden kann, dass einerseits keine unberechtigte Person Zugriff auf die Funktionen und Daten des DV-Systems erhält und andererseits für die berechtigten Personen die Menge der zugelassenen Operationen und das Profil der erlaubten Datenzugriffe bestimmt werden können[33]. Hierzu erfolgt bei jeder Kontaktaufnahme eines Benutzers mit dem DV-System eine Identifikation dieses Benutzers, z. B. durch Angabe seines Namens oder einer Nutzer-Kennung (Nutzer-ID). Durch den anschließenden Schritt der Authentisierung[34] wird dann sichergestellt, dass auch die korrekte Identität angegeben wurde. Hierzu überprüft das DV-System zusätzlich Informationen, die mit hoher Wahrscheinlichkeit nur der "echte" Benutzer liefern kann[35]:
Bei einer Authentisierung durch Wissen wird eine geheime Information abgefragt, die nur dem echten Benutzer zur Verfügung stehen sollte. Die am häufigsten benutzte Methode zur Identifizierung ist das Verfahren mit der persönlichen Identifikationsnummer (PIN), auch Geheimnummer oder Codenummer genannt.

33Weck, DuD 1995, 224, 224
34Authentisierung: Überprügung der Echtheit, Rechtsgültigkeit des Benutzers
35Weck, DuD 1995, 224, 224; vgl. dazu auch Rankl/Effing, 3. Aufl. 1999, S. 450 f.

Bei einer Authentisierung durch Besitz wird das Vorhandensein eines Objektes überprüft, das nur beim legalen Benutzer vorliegen sollte. Dies ist in der Regel ein maschinenlesbarer Ausweis, doch spielen hier auch oft mechanische Schlüssel die Rolle des authentisierenden Objekts. Schwachpunkt dieses Verfahrens ist, dass seitens des DV-Systems nicht überprüft werden kann, ob das betreffende Objekt, etwa durch Verleihen oder durch Diebstahl, in unechte Hände gelangt ist[36].

Während diese Verfahren bei zentralen Systemen inzwischen - zumindest theoretisch - beherrscht werden, bereiten sie im Rahmen der verteilten Datenverarbeitung, wie man sie bei Client/Server-Systemen hat, noch eine Reihe von Problemen:

Das Verfahren zur Authentisierung eines Benutzers sollte immer in gleicher Weise ablaufen, unabhängig davon, über welchen Weg er Zugang zum verteilten System erlangt. Es ist nicht zumutbar, beispielsweise bei Zugriff über verschiedene Rechner im Netz oder bei Zugriff auf verschiedene Server unterschiedliche Passwörter eingeben zu müssen. Andererseits erfordert die Verwendung desselben Passworts für alle Rechner im Netz, dass dieses Passwort überall dort bekannt ist, wo eine Authentisierung erfolgt; mithin wird eine sichere Übermittlung von Authentisierungsinformationen und ein Verfahren zur Konsistenswahrung dieser Informationen, beispielsweise bei einem Passwortwechsel, benötigt. Um den Gefahren durch Abhören des Datenverkehrs auf dem Netz und damit möglicherweise der Offenlegung von Passwörtern zu begegnen, ist es erforderlich, die Authentisierungsinformation verschlüsselt zu übermitteln

36Weck, DuD 1995, 224, 225

und/oder für jede Authentisierung neu zu erzeugen.

b)Zugriffs- und Funktionskontrolle durch Autorisierung

Ziel der Zugriffs- und Funktionskontrolle ist es zu verhindern, dass bei der Arbeit mit dem System generell berechtigte Personen Operationen und/oder Datenzugriffe ausführen, die außerhalb ihres Verantwortungsbereichs liegen (Autorisierung). In den gängigen Systemen wird die Zugriffskontrolle in der Regel matrixgesteuert durchgeführt, d. h. für jedes Paar (Benutzer, Schutzobjekt) lässt sich feststellen, ob eine bestimmte Operation zulässig ist oder nicht. So kann beispielsweise ein Subjekt ermächtigt werden, geschützte Daten oder Dienste zu nutzen. Dabei wird zwischen Lese-, Schreib-, Lösch- oder ausführendem Zugriff unterschieden[37]. Autorisierungsdienste leisten meist die Sicherheitsserver im Netzwerk.

c)Protokollierung des Zugangs

Auch ein im Prinzip sicherer Systembetrieb birgt in sich ein Element der Unsicherheit, wenn es nicht möglich ist nachzuweisen, dass die Systemsicherheit nicht verletzt, also keine unzulässigen Operationen durchgeführt oder vorbereitet wurden[38]. Aus diesem Grund muss ein DV-System, das den Anspruch der Sicherheit erhebt, Funktionen bereitstellen, mit denen nachgewiesen werden kann, welche Operationen von wem unter welchen

37Jäger, SINACARD 1999, S. 2
38Weck, DuD 1995, 224, 225

Umständen durchgeführt wurden. So muss es möglich sein festzustellen, welche Benutzer in welchen Zeiträumen mit dem System gearbeitet haben und von wo ihr Zugang erfolgte. Auch sollte es möglich sein, Einbruchsversuche zu erkennen, um gegebenenfalls den Eindringling in flagranti zu erwischen. Weiterhin sollte es möglich sein, auch die Zugriffe auf sensitive Datenbestände, zu denen insbesondere auch alle Konfigurationsdaten des Systems und die gespeicherten Bereichtigungsprofile gehören, überwachen zu können.

7. **Grenzen der klassischen Sicherheitskonzepte**

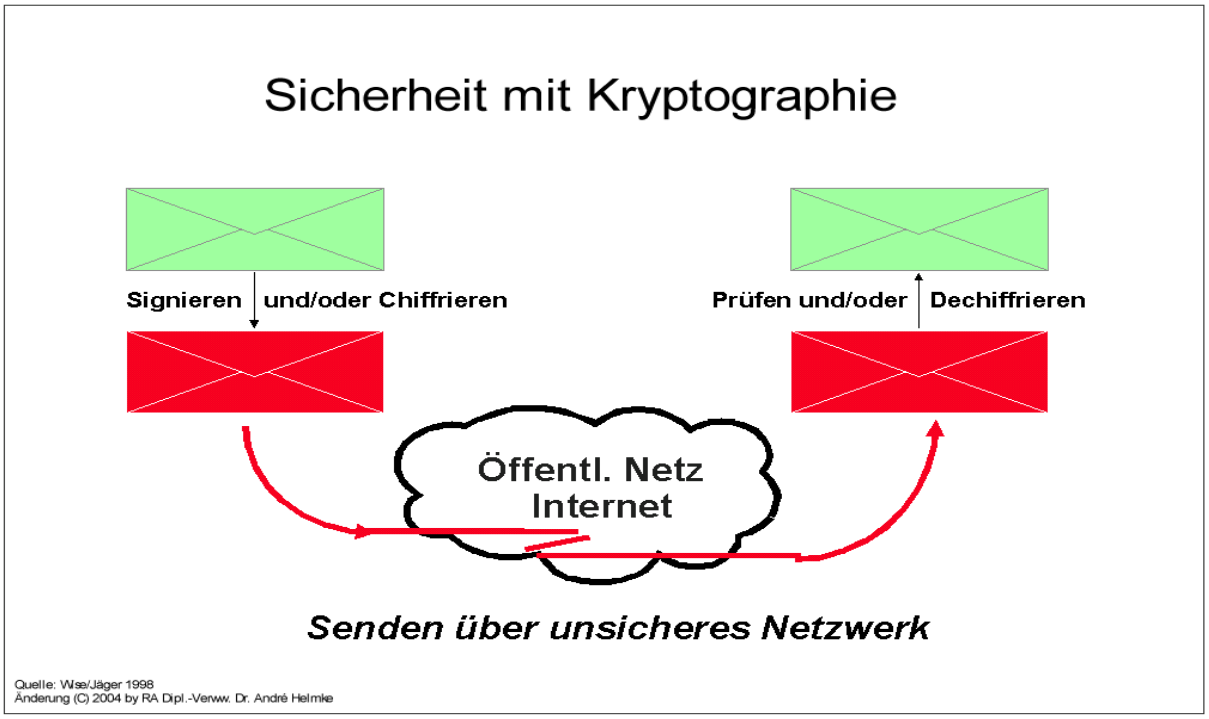
Die unverschlüsselte Übertragung von Passwörtern und PINs über das Internet ist ein konkretes Beispiel für die Grenzen der klassischen Sicherheitskonzepte. Durch die Abhörbarkeit der Passwörter und der PINs ist ihre Schutzwirkung in Frage gestellt. Auch vollkommen gutwillige Netzbenutzer, die auf legale Weise miteinander kooperieren, können aufgrund ihrer Kooperation in Konflikt miteinander stehen. Zur Absicherung ihrer Kommunikation fordern sie den Schutz vor einem nachträglichen Abstreiten ihrer Kommunikation durch den Partner. Um auch im offenen Netz verbindlich miteinander kooperieren zu können, müssen sie sich der Authentizität und Vertraulichkeit ihrer Kommunikation gewiss sein, und sie müssen die Ergebnisse ihrer Kooperation auch nachträglich gegenüber Dritten nachweisen können[39].

V. ***Einsatz von kryptographischen Verfahren***

39Grimm, DuD 1996, 27, 27

1. Die Kryptographie

Die Grenzen der klassischen Sicherheitskonzepte können und müssen mit Hilfe der Kryptographie geschlossen werden. Das Ziel dieser Untersuchung soll bekanntlich die sichere Versendung von Dokumenten im unsicheren Internet sein:



Unter Kryptographie wird im allgemeinen eine Verschlüsselung und Entschlüsselung der Daten zur Geheimhaltung verstanden[40]. Verschlüsseln bedeutet: Umwandeln eines Textes (d. h. einer Folge von Zeichen aus einem Alphabet) in einen solchen (wobei

40Ausführlicher dazu bei Schäfer, 1997, S. 64 ff.

meist das Alphabet das gleiche bleibt) nach Maßgabe einer festen Rechenvorschrift (eines "Algorithmus"), wobei diese jedoch parametisiert wird durch eine veränderliche Größe, den sog. "Schlüssel"[41].

2. **Das Schlüsselmanagement**

Eine noch so gut abgesicherte Wohnungstür hilft nicht, wenn der Schlüssel in unbefugte Hände gerät. Wird der Schlüssel beispielsweise auf der Festplatte eines Computers gespeichert, so kann er ausgelesen, kopiert und von Unbefugten verwendet werden. Auch das Signaturgesetz akzeptiert dies nicht. Wie versteckt man also diesen sog. "Schlüssel" am besten?
Gängig ist zur Zeit, die Geheimschlüssel mit einem Passwort überschlüsselt auf dem lokalen PC des Inhabers abzuspeichern in einer sogenannten "Personal Security Environment"[42]. Der Nachteil ist, dass es nicht verhindert werden kann, dass ein Unbefugter sich diesen Schlüssel über das Netz holt. Für Behörden und Gerichte ist dieses Risiko nicht hinnehmbar.

Als Versteck bietet sich nun die Smartcard an. Smartcards sind ein ideales Mittel, um Schlüssel zu speichern und zu verwalten. Wenn ein Schlüssel einmal gespeichert ist, muss er nie mehr außerhalb der Karte aufbewahrt werden. Der Geheimschlüssel kann auch auf der Smartcard erzeugt werden. Er ist damit hardware-geschützt. Die Smartcard ist mobil, der Nutzer kann sich frei

41Heuser, HMD 190/1996, 8, 9
42Jäger, 1997, S. 13

bewegen und immer seine Sicherheits-Identität mitführen. Die Smartcard wird somit zum virtuellen Schlüssel, den man wie einen Wohnungsschlüssel in die Hand nehmen und auch ähnlich verstecken kann[43].

Die Smartcard ermöglicht damit ferner ein äußerst qualifiziertes PIN-Verfahren: Die PIN muss nicht mehr über Leitungen gesandt und von einem Rechner geprüft werden. Die PIN wird auf der Tastatur eines Terminals oder Computers eingegeben und dann zur Smartcard gesendet. Diese vergleicht den übergebenen Wert mit einem gespeicherten Referenzwert und teilt dann das Ergebnis dem Terminal mit. Die besonderen Tastaturen verschlüsseln die PIN unmittelbar bei der Eingabe. Damit wird zuverlässig verhindert, dass ein Angreifer diese Tastatur manipulieren und die PIN während der Eingabe abhören kann[44].

3. **Kryptographie mit der Smartcard**

Ein wesentlicher Vorteil der Smartcard gegenüber anderen Identifikationskarten wie z. B. der Magnetkarte ist, dass man in ihr Daten nicht nur speichern, sondern auch verschlüsseln kann. Dabei findet der gesamte Datenaustausch zwischen Terminal und Smartcard durch digitale elektrische Impulse über die I/O-Leitung der Smartcard statt.
Es ist vorstellbar und auch technisch einfach realisierbar, mit einem an dem I/O-Kontaktfeld angelöteten Draht die gesamte

43Wise/Jäger, 1998, S. 19
44Rankl/Effing, 3. Aufl. 1999, S. 452

Kommunikation aufzuzeichnen und später zu analysieren[45]. Diese Angriffe würden nur dann zu einem Erfolg führen, wenn geheime Daten ungesichert über die I/O-Leitung gingen. Um nun solche Angriffe abzuwehren, gibt es verschiedene kryptographische Algorithmen.

Kryptographische Algorithmen sind nach mathematischen Gesetzmäßigkeiten aufgebaut (Einwegfunktion, Modulo-Arithmetik usw.). Es gibt symmetrische Systeme, bei denen beide Teilnehmer über denselben Schlüssel verfügen (z. B. DES = Data Encryption Standard) und asymmetrische Systeme (z. B. RSA nach den Erfindern Rivest, Shamir, Adleman), bei denen jeder Teilnehmer ein Schlüsselpaar, bestehend aus einem privaten Schlüssel (sog. Privat-Key) und einem öffentlichen Schlüssel (sog. Public-Key), erhält[46]. Die Rücktransformation einer verschlüsselten Information ohne Kenntnis des Schlüssels ist auch bei bekanntem Algorithmus nicht möglich.

Hinsichtlich der Geheimhaltung des Schlüssels sind also zwei logisch verschiedene Verfahren zu unterscheiden:

a)Symmetrische Verschlüsselung

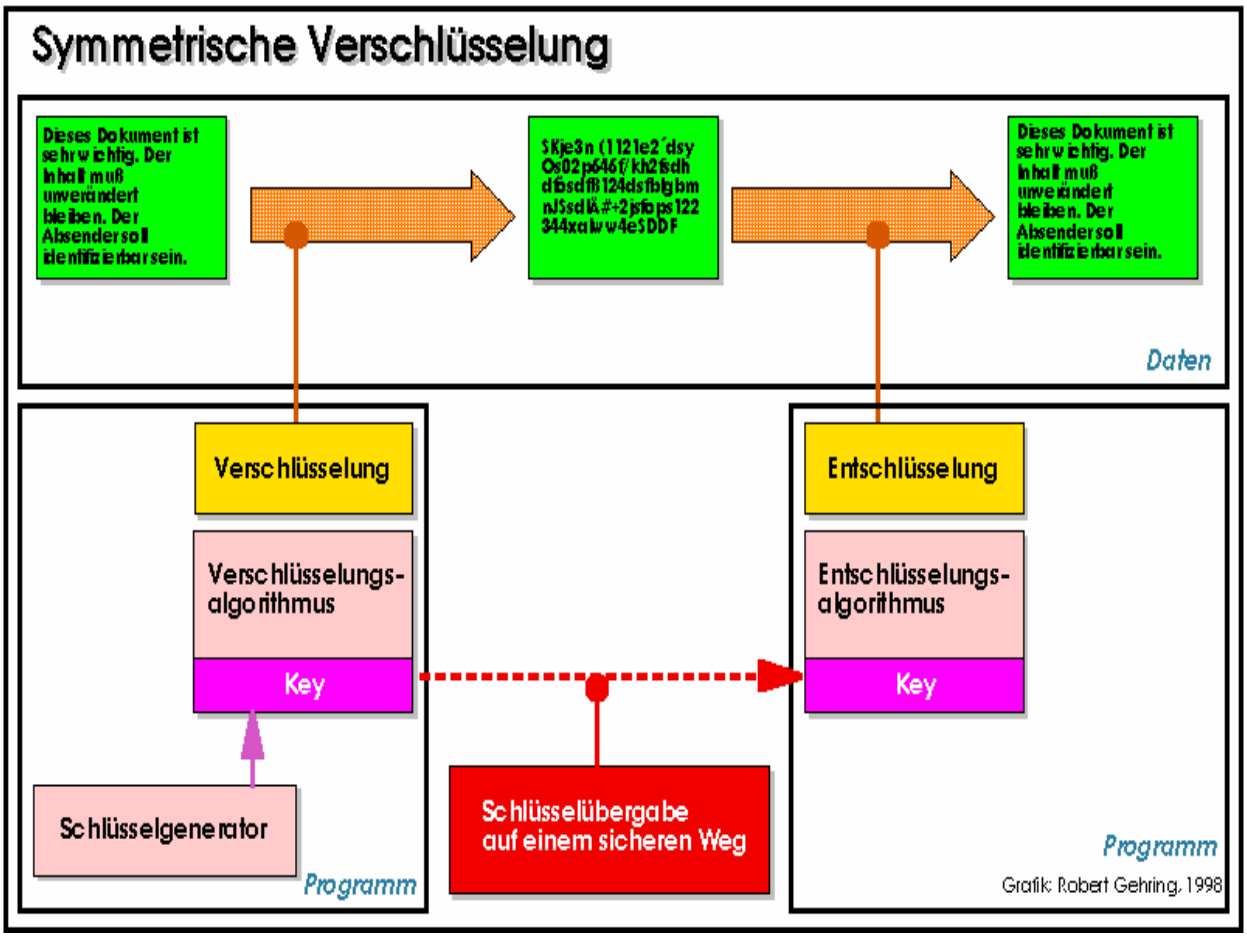
Sogenannte "symmetrische" Verschlüsselungsverfahren sind dadurch gekennzeichnet, dass jeder Benutzer ("Absender" und "Empfänger" einer Nachricht) über einen gemeinsamen Schlüssel verfügt, der sowohl der Ver- wie der Entschlüsselung dient und unter allen Umständen geheim zu halten ist und tunlichst auf irgendeinem

45Rankl/Effing, 3. Aufl. 1999, S. 381
46Kruse/Peuckert, DuD 1995, 142, 145

sicheren Wege ausgetauscht werden muss.

Der Phantasie sind beim Entwurf solcher Verfahren kaum Grenzen gesetzt; es sind in den letzten Jahren auch eine Reihe solcher Algorithmen publiziert worden (DES, IDEA, FEAL SAVER, ...), die - in unterschiedlich kryptographischer Qualität - Daten in sehr hohen Raten (bis zu einigen Hundert Megabit/Sekunde) zu verschlüsseln gestatten.

Es ist die Stärke der symmetrischen Verfahren, vergleichsweise leicht in Hard- und Software implementierbar zu sein und eben auch sehr hohe Verschlüsselungsgeschwindigkeiten zu erlauben; ihre Crux liegt in der Notwendigkeit der gesicherten Verteilung geheimer Schlüssel[47].



Der Hauptnachteil des symmetrischen Verfahrens besteht darin, dass Sender und Empfänger den gleichen Schlüssel benutzen müssen. Das erfordert eine strikte Geheimhaltung des Schlüssels.

47Heuser, HMD 190/1996, 8, 10

Außerdem lässt sich der geheime Schlüssel ermitteln, wenn man die Daten und das Ergebnis der Verschlüsselung kennt. Wird schließlich innerhalb einer Benutzergruppe derselbe Schlüssel benutzt, kann der Schlüssel nicht zur Unterscheidung verwendet werden. Innerhalb einer solchen Gruppe "kann es jeder gewesen sein"[48]. Deshalb ist diese Art der Identifikation nach außen nicht beweisbar. Ein Richter wird nicht entscheiden können, wer aus der Benutzergruppe den Schlüssel verwendet hat. Deshalb kann man symmetrische Verfahren nur in solchen Umgebungen einsetzen, in denen schon ein hohes Maß an Vertrauen besteht.

b)Asymmetrische Verschlüsselung

Die mathematische Kryptograpie hat einen enormen Aufschwung erfahren durch das Paradigma der asymmetrischen oder "public-key"-Verfahren, entdeckt um 1975. Diese Idee beruht auf dem Gedanken der "Einbahnfunktion", einer mathematischen Funktion nämlich[49], die zwar leicht auszuwerten ist, deren Umkehrfunktion jedoch nur bei Kenntnis einer bestimmten Zusatzinformation berechenbar ist[50].

Zur Ver- und Entschlüsselung von Daten werden zwei unterschiedliche, aber zusammengehörende Schlüssel benutzt. Ein Schlüssel, der geheimgehalten werden muss, wird Privat-Key (privater Schlüssel) genannt. Der zweite Schlüssel kann ohne Bedenken veröffentlicht werden und wird Public-Key (öffentlicher Schlüssel) genannt. Die Idee hinter einem Privat/Public-Key-

48Grimm, DuD 1996, 27, 28
49Näheres dazu vgl. Münzenberger, HMD 190/1996, 31 ff.
50Heuser, HMD 190/1996, 8, 10

Algorithmus ist, dass man die Daten mit einem Schlüssel verschlüsselt und mit dem anderen entschlüsselt[51].
Daraus entsteht auf folgende Weise ein Chiffrierverfahren: der Empfänger einer Nachricht stellt dem Absender eine solche Einbahnfunktion offen zur Verfügung (und hält die entscheidende Zusatzinformation geheim); der Absender verschlüsselt seine Nachricht mittels der ihm bekannten Einbahnfunktion. Entscheidender Vorteil eines solchen Modells ist, dass hier keinerlei geheime Informationen - etwa auf dem Kurierwege - transportiert werden müssen !

aa)**RSA**

Es ist das Verdienst von Diffie und Hellmann, erkannt zu haben, dass eine Verschlüsselungstechnik in offenen Netzen erst dann sicher benutzt werden kann, wenn man die zugehörigen geheimen Schlüssel nicht mehr über das Netz kommunizieren muss[52]. Die Idee von Diffie und Hellmann war es, Verschlüsselungsverfahren zu entwerfen, die man nur dadurch knacken kann, dass man ein bisher ungelöstes mathematisches Problem löst, z. B. das Faktorisieren einer großen Zahl oder die Berechnung eines diskreten Logarithmus mit Hilfe eines "schnellen" deterministischen Algorithmus[53]. Solche Algorithmen kennt bisher niemand, und ob es solche gibt, ist ungewiss.
Allerdings ist es alles andere als einfach, solche bedingt umkehrbaren Einbahnfunktionen zu finden; sehr bekannt geworden

51Volpe/Volpe, 1996, S. 60
52Grimm, DuD 1996, 27, 28 m.w.N.
53Grimm a.a.O.

ist das RSA-Verfahren (nach den Autoren Rivest, Shamir und Adleman), das von der mathematischen Schwierigkeit der Zerlegung großer Zahlen in ihre Primfaktoren Gebrauch macht[54]. Daneben hat später ElGamal (ELGA) die Forderung von Diffie und Hellmann konkretiersen können[55].

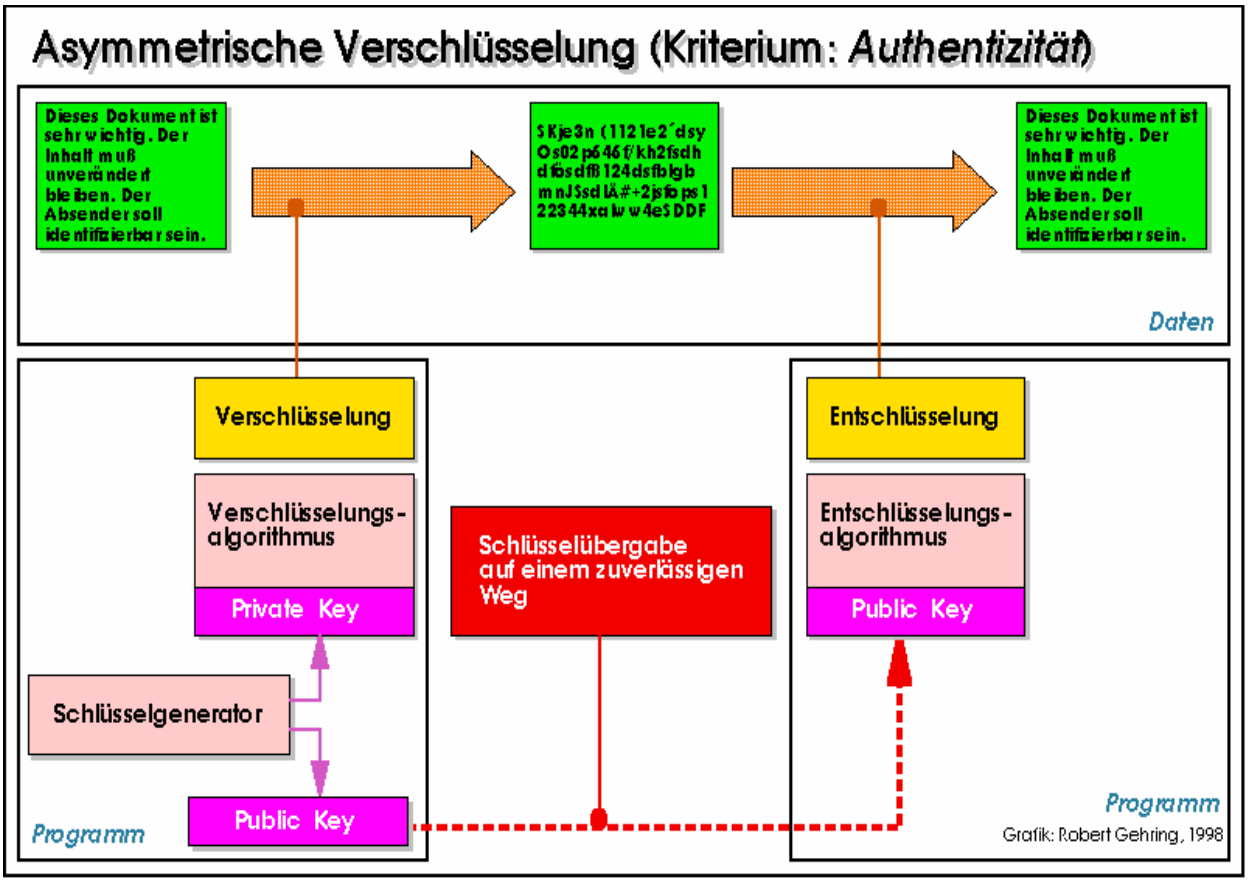
Beide Verfahren gelten heute als sicher in dem Sinne, dass man annimmt, dass ihre Sicherheit wirklich auf dem Problem der Faktorisierung bzw. dem des diskreten Logarithmus beruht[56].

Der RSA-Algorithmus ermöglicht drei verschiedene Anwendungen: zum einen das Authentifizieren eines Datensatzes mit Hilfe der sogenannten "Digitalen Signatur", zum anderen die Identifizierung der Nutzer durch Authentisierung und schließlich das Verschlüsseln eines Datensatzes zum Zwecke des Verbergens vor Unbefugten.

Ein großer Nachteil aller asymmetrischen Verfahren ist ihre hohe Berechnungskomplexität - dies kann auch nicht anders sein, da auf andere Weise kaum Einbahnfunktionen entstehen können[57].

Soll beispielsweise sichergestellt werden, dass der Schriftsatz auch tatsächlich von dem Rechtsanwalt Meier stammt, so müsste das Dokument wie folgt verschlüsselt werden:

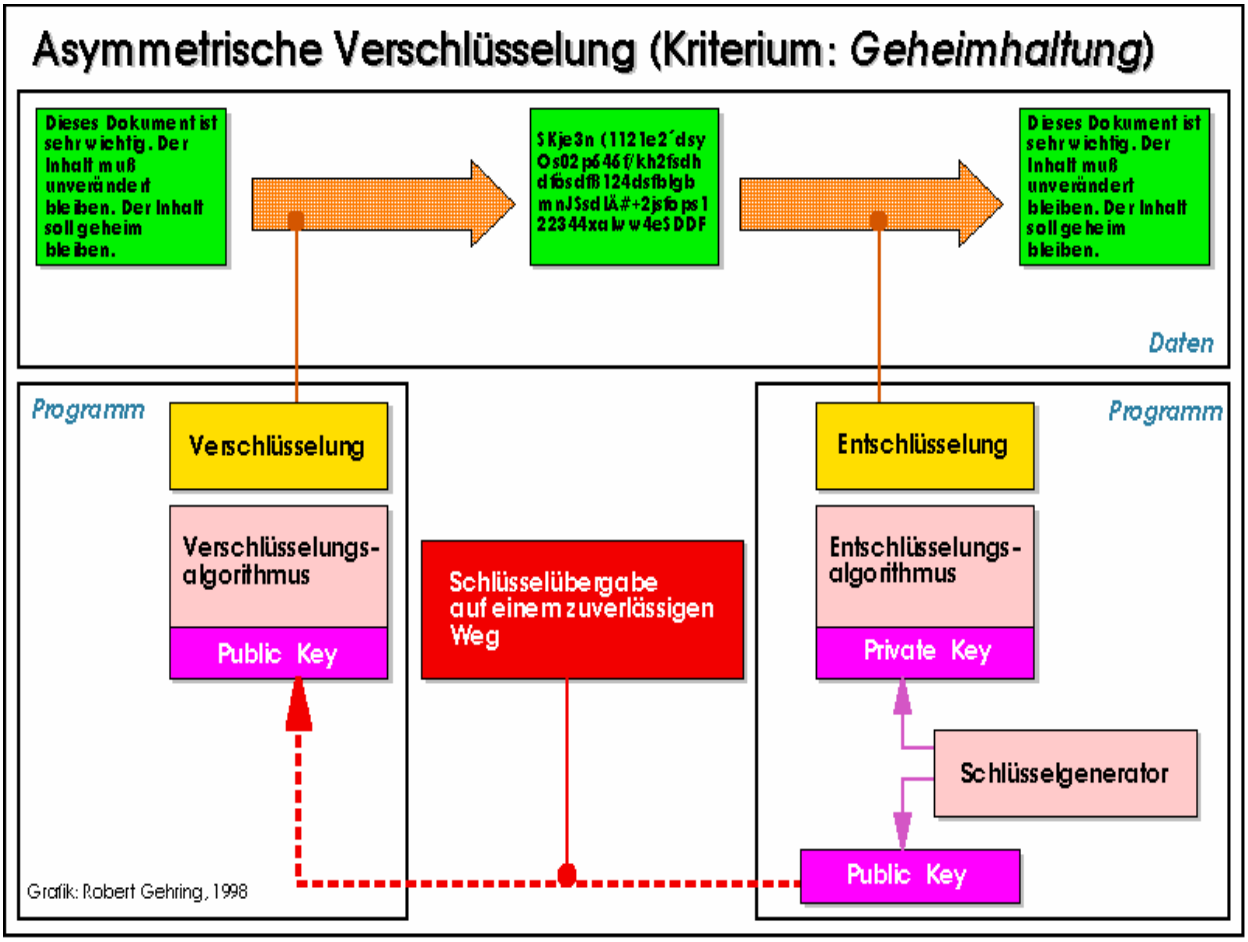
54Heuser, HMD 190/1996, 8, 11
55Grimm, DuD 1996, 27, 28 m.w.N.
56Grimm, DuD 1996, 27, 28
57Heuser, HMD 190/1996, 8, 11



Da das Dokument mit dem Private-Key des Rechtsanwaltes Müller verschlüsselt worden ist, kann das Gericht einwandfrei die Herkunft des Dokumentes überprüfen. Der Nachteil hierbei ist jedoch, dass jeder, der den Public-Key des Rechtsanwaltes Müller kennt, das Dokument auch lesen kann. Um die Vertraulichkeit des Dokumentes zu gewährleisten, bedarf es mithin einer zusätzlichen Verschlüsselung auch des Inhaltes des Dokumentes.

Soll demgegenüber ein Dokument nur einem bestimmten Adressaten zugesandt werden, und soll auch nur dieser (z. B. das Gericht)

das Dokument lesen können, so wird das Dokument wie folgt verschlüsselt werden müssen:



Da das Dokument lediglich mit dem Publik-Key des Gerichts verschlüsselt worden ist, kann das Gericht nicht einwandfrei die Herkunft des Dokumentes überprüfen. Jeder, der den Publik-Key des Gerichts besitzt, könnte dem Gericht das Dokument zugesandt haben. Aber durch dieses Verschlüsselungsverfahren des Dokumentes ist sichergestellt worden, dass ausschließlich das Gericht mit seinem Private-Key das Dokument wird lesen können.

bb)**Digitale Signatur (Elektronische Unterschrift)**

Durch den Einsatz des RSA wurde die Möglichkeit einer elektronischen Unterschrift, auch digitale Signatur genannt, erst geschaffen. Eine digitale Signatur im Sinne des Signaturgesetzes ist gem. § 2 Abs. 1 SigG ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde nach § 3 SigG versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt. In den meisten Fällen kommt es weniger darauf an, die Daten zu verschlüsseln (der RSA-Algorithmus ist nicht so sehr dafür entwickelt worden), sondern man möchte sicher sein, dass die Daten nicht verändert oder verfälscht worden sind[58]. Weiter ist es wichtig, die Authentizität der Daten zu bestätigen.

(1)*Prüfsumme mit dem Hash-Verfahren*

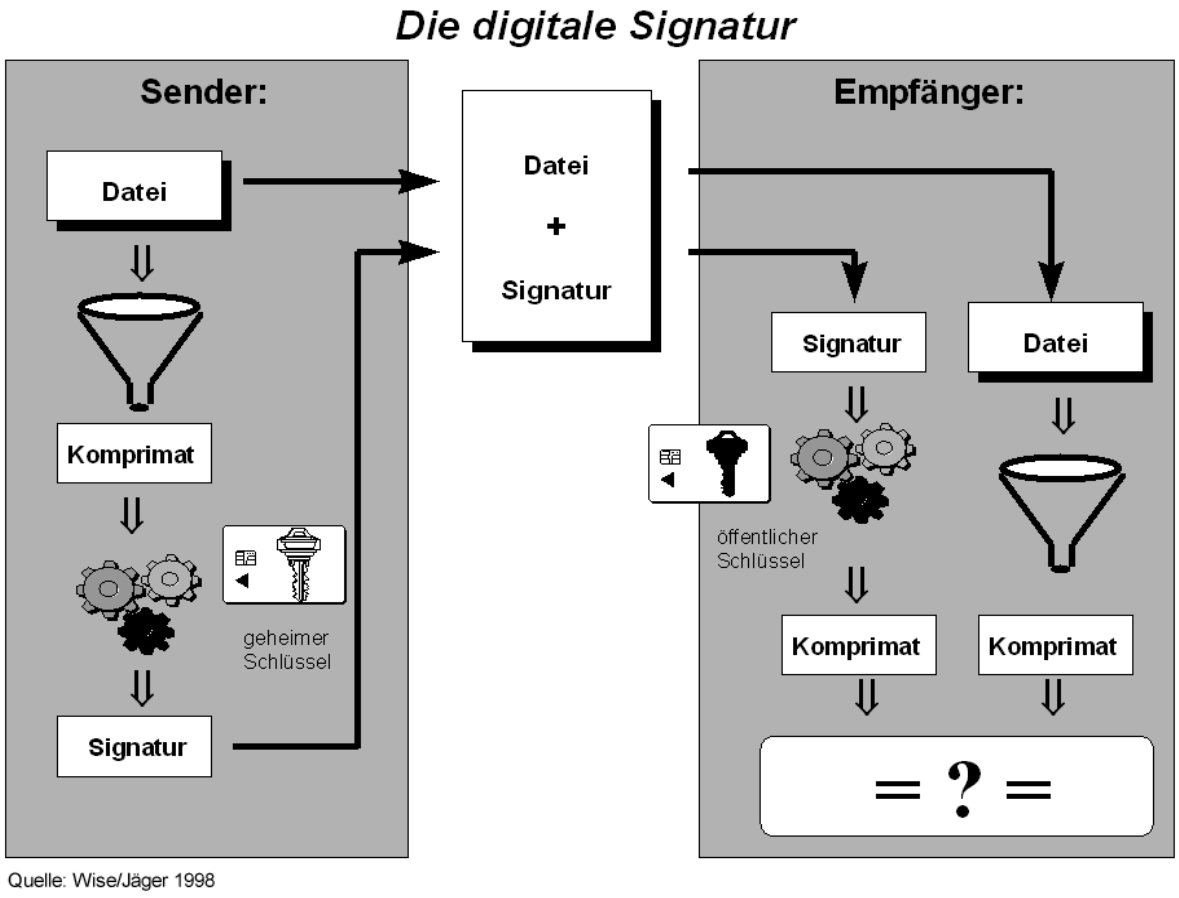
Bei der Berechnung der elektronischen Unterschrift werden nicht alle Daten mit dem RSA-Algorithmus verschlüsselt, sondern die Daten werden erst einer Hash-Funktion unterzogen. Diese liefert einen sogenannten Hash-Wert, ähnlich einem CRC-Prüfzeichen[59], der sich mit großer Sicherheit verändert, falls die Daten

58Volpe/Volpe, 1996, S. 63
59Vgl. dazu auch Volpe/Volpe, 1996, S. 54 ff.; Schäfer, 1997, S. 82 f. und Kruse/Peuckert, DuD 1995, 142, 146

manipuliert wordern sind[60]. Statt der gesamten Daten wird nur der Hash-Wert mit dem RSA-Algorithmus verschlüsselt. Der geheime Schlüssel des RSA befindet sich in einer Smartcard. Anschließend werden die Daten und der verschlüsselte Hash-Wert über eine Leitung, z. B. ein öffentliches Netz, übertragen. Am anderen Ende der Leitung werden die Daten mit dem verschlüsselten Hash-Wert wieder empfangen. Hätte man nur die Daten, so könnte man weder auf die Datenechtheit noch auf die Quelle schließen.

60Volpe/Volpe, 1996, S. 64

Die folgende Abbildung verdeutlicht das Ergebnis des Hash-Verfahrens als "Komprimat":

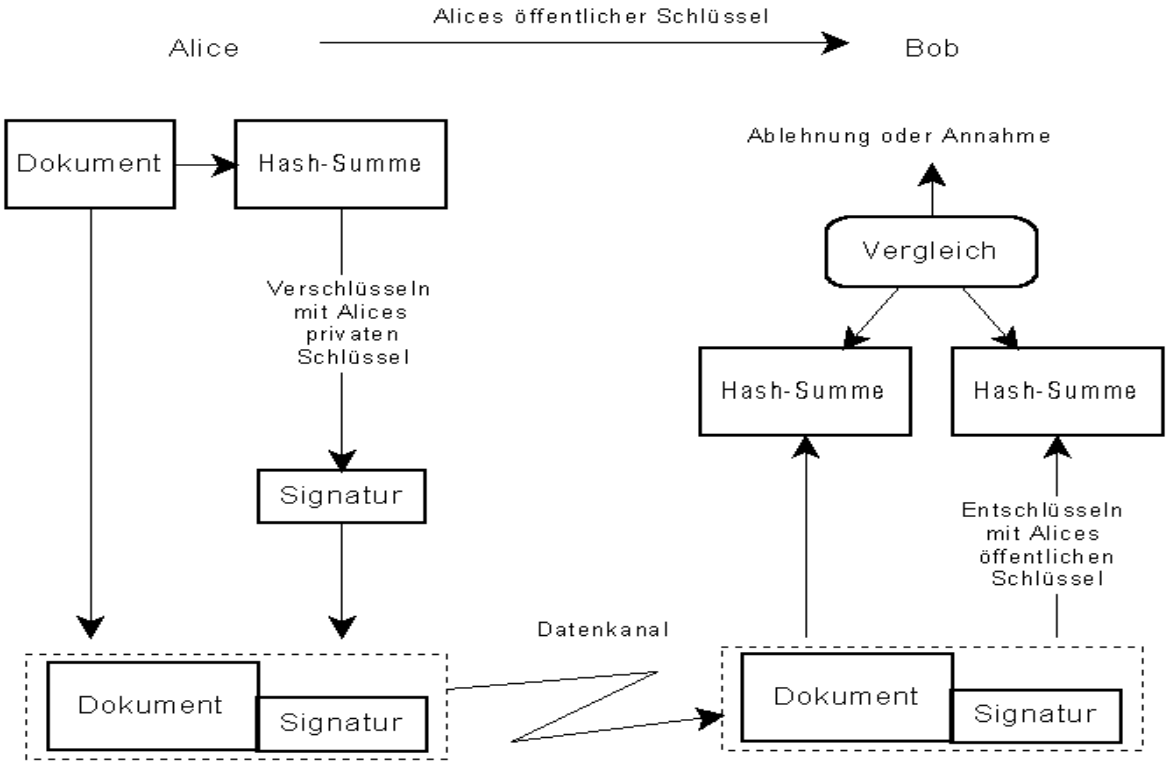


(2)*Überprüfung der Digitalen Signatur*

Wie sieht es mit der Originalität des Dokumentes aus? Kommt das Dokument tatsächlich von dem Absender, der genannt ist? Ist das Dokument authentisch? Ja, das ist der Fall: Der Absender hat das Dokument mit seinem persönlichen Geheimschlüssel verschlüsselt.

Wenn das Dokument mit dem zugehörigen öffentlichen Schlüssel geöffnet werden kann, ist bewiesen, dass es nur von dem besagten Absender stammen kann.

Der Empfänger entschlüsselt nun mit dem passenden öffentlichen Schlüssel den erhaltenen Hash-Wert und berechnet separat den Hash-Wert der emfangenen Daten. Nur wenn beide Ergebnisse übereinstimmen, sind die Daten nicht manipuliert worden, und der Empfänger kennt die Identität der Quelle.



Unterzeichnen mit Einweg-Hashfunktion und RSA

Vorausgesetzt wird dabei, dass die Bindung "Public-Key (Öffentlicher Schlüssel) - Private-Key (Geheimer privater Schlüssel)" zu einer Person echt ist. Dies wird nachgewiesen durch das Signaturschlüssel-Zertifikat. Es ist die Beglaubigung, dass ein Public-Key und ein Private-Key und eine bestimmte Person

(Smartcard-Besitzer) zusammengehören.
Der Private-Key ist das wichtigste und zugleich am meisten gefährdetete Glied in der Sicherheitskette. Was wäre besser geeignet als die Smartcard, um Private-Keys abzuspeichern und aufzubewahren?

cc)**Authentisierung mit dem RSA-Verfahren**

(1)*Fallbeispiel "Führerscheinantrag"*

Zur Verdeutlichung der Anwendung von Smartcards und der Feststellung der Authentizität soll das folgende Beispiel dienen: Eine Stadt bietet ihren Bürgern an, über das World-Wibe-Web einen Führerschein zu beantragen. Dabei entstehen im wesentlichen zwei Probleme: Erstens muss die Stadt sichergehen, dass der Bürger tatsächlich derjenige ist, der er vorgibt zu sein. Zweitens müssen die Bürgerdaten, wie Name, Geburtsdatum, Anschrift, der Stadt codiert übers Internet übermittelt werden, da sonst die Gefahr des Abhorchens besteht. Zu diesem Zweck enthält jeder Bürger eine eigene Smartcard, in der ein Privat-Key sicher abgelegt ist. Der Bürger kann mit dieser Smartcard seinen Führerscheinantrag verschlüsseln und über das Netz an die Stadt senden. Bei der Führerscheinstelle der Stadt kann mit dem passenden Public-Key der Antrag des Bürgers entschlüsselt werden. Da dieser Public-Key nur zum Privat-Key eines bestimmten Bürgers passt, ist gleichzeitig die Identität des Bürgers geprüft worden.
Zur Durchführung der Authentifikation benötigt die Stadt aber

den öffentlichen Schlüssel der Smartcard. Da dieser Schlüssel nicht geheim ist, kann er in einem öffentlichen Verzeichnis (Directory) gespeichert sein oder er kann vor bzw. im Rahmen der Authentifikationsprozedur offen übertragen werden. Es wird hierbei unterstellt, dass die öffentlichen Schlüssel authentisch sind[61].

(2)*Das Challenge-Response-Verfahren*

Für die Überprüfung, inwieweit der übermittelte Public-Key und der Private-Key auf der Smartcard zusammengehören, bietet sich das sogenannte Challenge-Response-Verfahren an.
Das Challenge-Response-Verfahren basiert auf einem sehr logischen Frage-Antwort-Verfahren, bei dem die Partner (auch ein Rechner und ein Benutzer) ein gemeinsames Geheimnis haben[62]. Nur wer dies kennt, kann auf eine Frage die richtige Antwort geben. Damit das Geheimnis nicht "abgehört" werden kann, erfolgt beim Challenge-Response-Verfahren die Echtheitsprüfung dynamisch, d. h. mit sich ständig ändernden Werten. Dazu sendet der Rechner beispielsweise eine unverschlüsselte Zufallszahl an die Smartcard, die vom Chipkartenprozessor mit dem im EEPROM gespeicherten geheimen Schlüssel nach dem RSA-Verfahren verschlüsselt wird. Das sich daraus ergebende Chiffrat wird an den Rechner übertragen und dort nach demselben Schema - unter Hinzuziehung des passenden öffentlichen Schlüssels - entschlüsselt. Der so entstandene Klartext wird mit der zuvor

61Mehr dazu später unter dd).
62Kruse/Peuckert, DuD 1995, 142, 145

erzeugten Zufallszahl verglichen. Nur bei Übereinstimmung verfügt die Smartcard über den passenden Geheimschlüssel (Privat-Key). Da sich die Zufallszahl bei jedem Authentisierungsvorgang ändert, ergibt sich jedesmal ein anderer Parameter. Damit kann der Geheimschlüssel auch beim Abhören des Authentisierungsvorganges nicht analysiert werden.
Mit dem Challenge-Response-Verfahren kann somit zweifelsfrei die Identität des Benutzers festgestellt werden.
Umgekehrt ist es auch möglich, das System zu authentisieren. Dazu stellt die Smartcard dem System eine Frage, wartet auf dessen Antwort und vergleicht beide Ergebnisse miteinander[63].
Um sicherzustellen, dass auch die korrekte Identität angegeben wurde oder anders ausgedrückt, dass auch der Private-Key samt Smartcard und der Benutzer zusammengehören, wird der Smartcardinhaber anschließend aufgefordert, seine persönliche Identifikationsnummer (PIN) einzugeben[64].

(3)*Fallbeispiel Online-Kommunikation Rechtsanwälte - Gerichte*

Rechtsanwalt Meier hat von seiner Mandantin den Auftrag erhalten, eine Auflassungsklage (= Klage auf Übereignung eines Grundstücks) für ein Haus, welches sie im Internet bei eBay für 2,50 EUR[65] ersteigert hat, zu erheben. Er fertigt die Klageschrift auf seinem Computer. Den Schriftsatz unterschreibt er elektronisch d. h., er signiert ihn mit seiner Smartcard, um durch diese Verschlüsselung die Authentizität der Klageschrift

63Volpe/Volpe, 1996, S. 109
64So wohl auch JKomG-BReg, Seite 55
65Siehe dazu FAZ vom 06.08.2004, Seite 7

sicherzustellen. Und so könnte die Kommunikation zwischen Rechtsanwalt Meier, seiner Smartcard und dem zuständigen Gericht funktionieren:

(a)Der Client (Computer des Rechtsanwaltes) nimmt die Verbindung zum Server (Computer) des Gerichts auf. Anschließend klickt Rechtsanwalt Meier im Internet auf der Homepage des zuständigen Gerichts den "Gerichtsbriefkasten" an. Zunächst wird das Gericht im Rahmen des "Log-on" den Benutzernamen und das Passwort des Rechtsanwaltes Meier abfragen, um überhaupt einen "allgemeinen Zugriff" auf den Gerichtsserver zu gestatten.

(b)Für einen Vollzugriff[66] auf den Server des Gerichts sendet das Gericht nun eine Identifikationsanfrage mit einer unverschlüsselten Zufallszahl an den Client[67].

(c)Der Client übermittelt die Anfrage an die Smartcard.

(d)Mit Hilfe einer Kodierung konstruiert die Smartcard eine digitale Unterschrift mit der unverschlüsselten Zufallszahl für die Anfrage. Dieser Schlüssel kann weder durch Viren verändert noch von Programmen geknackt werden, da die Codierung nicht vom Computer, sondern von der Smartcard selbst verarbeitet wird.

(e)Die Smartcard leitet die unterschriebene Anfrage zurück an

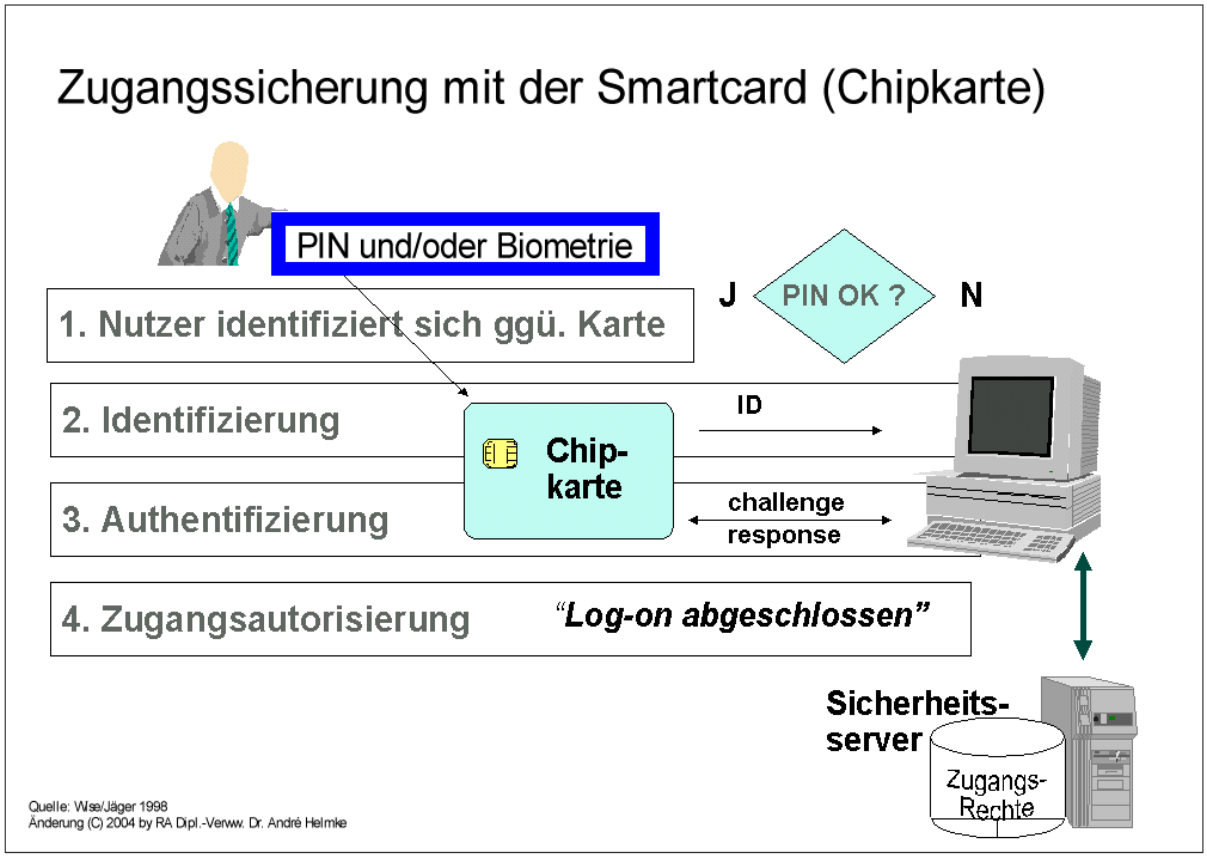
66Da in Zukunft Rechtsanwälte/Innen und Notare/Innen einen Vollzugriff auf den Gerichtsserver erhalten sollen, ist meines Erachtens dieses Verfahren zwingend notwendig.
67Siehe näheres oben zum Challenge-Response-Verfahren

den Client.

(f)Der Client schickt die Antwort auf die Anfrage an den Server des Gerichts zurück.

(g)Der Server des Gerichts kontrolliert die Gültigkeit der Unterschrift und gewährt noch korrekter Identifikation den Vollzugang zum Gerichtsserver.

Bis hierhin können die obigen Schritte grafisch wie folgt dargestellt werden:

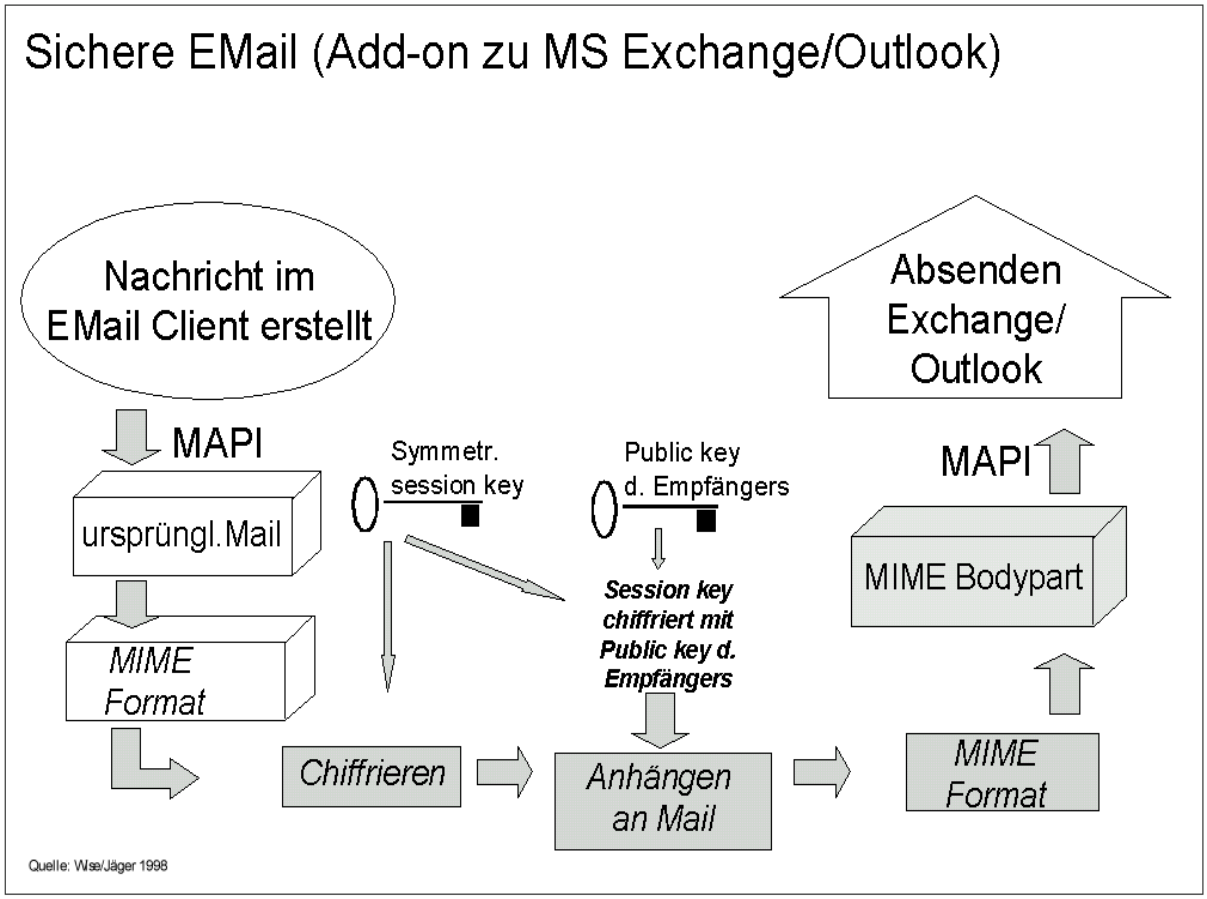


(h)Im nächsten Schritt klickt Rechtsanwalt Meier die Option "Neues Verfahren" auf dem Server des Gerichts an und fügt in das Feld "Wählen Sie das zu übertragende Dokument" das Dokument "Klageschrift" ein. Anschließend klickt er den Button "Übertragen" an und übermittelt so mit dem Webbrowser den elektronischen Schriftsatz per Upload.

Eine Verschlüsselung des Schriftsatzes könnte beispielsweise mit

TrustedMIME von Siemens Nixdorf erfolgen.

Die folgende Abbildung stellt prinzipiell dar, wie eine E-mail behandelt wird, wenn TrusedMIME in Exchange oder Outlook eingehängt ist:



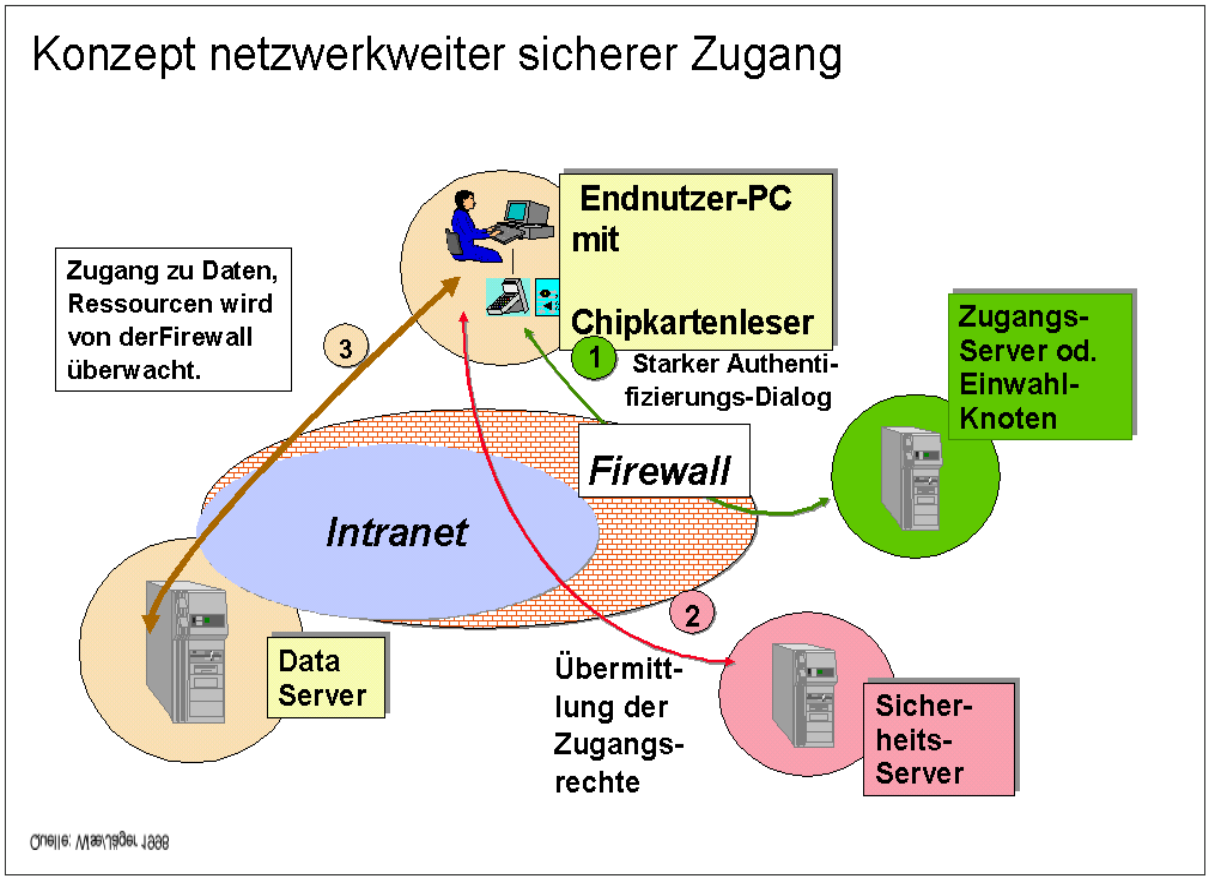
(i)Der Server des Gerichts empfängt den elektronischen Schriftsatz des Rechtsanwaltes Meier und überprüft den Hash-Wert, damit Änderungen des Schriftsatzes im Internet ausgeschlossen werden können. Wird das Dokument selbst nicht verschlüsselt, besteht die Gefahr, dass es von jedem im Netz gelesen werden kann. In diesem Falle sollte sich der

Rechtsanwalt von seiner Schweigepflicht - soweit hierzu erforderlich - entbinden lassen oder aber auch das Dokument selbst verschlüsselt übersenden (siehe weiter unten zum **Hybridverfahren**).

(j)Der Server des Gerichts sendet eine Eingangsbestätigung an den Client, die per E-mail bei Rechtsanwält Meier eingeht. Damit kann er kontrollieren, ob sein Schriftsatz tatsächlich bei Gericht eingegangen ist.

(k)Das Dokument wird unveränderbar in der elektronischen Akte des Gerichts gespeichert. Über Zustellungen an den Beklagten oder andere Prozessparteien wird der Rechtsanwalt Meier elektronisch informiert. Um sich über den aktuellen Verfahrensstand zu informieren, kann Rechtsanwalt Meier jederzeit online vom Schreibtisch seiner Kanzlei aus in der elektronischen Gerichtsakte blättern. Der parallele Zugriff ist in diesem Stadium besonders interessant, da Richter die Akte zur Vorbereitung auf den Prozess mehrfach anfordern und weitere Verfügungen treffen. Zusätzlich kann der Richter Bevollmächtigten gestatten, auf den elektronischen Bestand zuzugreifen. Hierdurch entfällt das Erstellen von Abschriften durch die Geschäftsstelle und Kosten für deren Versand.

Das Sicherheitskonzept des Gerichts könnte abschließend grafisch wie folgt dargestellt werden:



dd)**Zertifizierung öffentlicher Schlüssel**

Sicherheitskonzepte, die Kryptographie benutzen, benötigen eine Schlüsselverwaltung. Dies gilt insbesondere für die asymmetrische Authentisierung und für die Digitale Signatur. Dabei muss sichergestellt werden, dass der öffentliche Schlüssel auch tatsächlich authentisch ist, d. h. demjenigen wirklich gehört,

der sich als Inhaber ausgibt[68].

Diese Bindung geschieht durch einen (glaubwürdigen) Text, der aussagt: Der öffentliche Schlüssel sowieso (wörtliches Zitat seiner Bitfolge) gehört zur Person sowieso (wörtliches Zitat des Besitzernamens)[69]. Dieser Text kann entweder in Form eines "elektronischen Zertifikats" von einer "Zertifizierungsinstanz" signiert sein, oder er kann zur "Vorstellung" einer unbekannten Person formuliert und ggf. unmittelbar überprüft werden.

Wie können nun Zertifikate über öffentliche Schlüssel und Personennamen gestaltet sein, damit sie glaubwürdig verifizierbar sind? Es haben sich zwei grundsätzlich verschiedene Modelle für die auhentische Bindung öffentlicher Schlüssel an ihre Besitzer herausgebildet, zum einen nach dem PEM-Verfahren und zum anderen nach dem PGP-Verfahren.

(1)*PEM-Verfahren*

Dies wird beispielsweise erreicht durch ein besonderes Verfahren zur Beglaubigung von öffentlichen Schlüsseln, "Zertifikate" genannt. Sogenannte Zertifizierungsstellen (engl. Certification Authorities - CA - oder auch Trust Center genannt) belaubigen öffentliche Schlüssel[70]. Gemäß § 2 Abs. 2 SigG ist eine Zertifizierungsstelle im Sinne des Signaturgesetzes eine natürliche oder juristische Person, die die Zuordnung von öffentlichen Signaturschlüsseln zu natürlichen Personen bescheinigt und dafür eine Genehmigung gemäß § 4 SigG besitzt.

68Wise/Jäger, 1998, S. 12
69Grimm, DuD 1996, 27, 31
70Wise/Jäger, 1998, S. 12

In den vergangenen Jahren hat eine Internet Engineering Task Force Erweiterungen der einfachen Internet-Nachrichtenformate spezifiziert, die als "Privacy Enhanced Mail" (PEM) bezeichnet werden[71]. Eine Besonderheit der PEM-Spezifikation ist ihre Konkretisierung eines Zertifzierungsverfahrens. Sie schlagen ein in vier Funktionsstufen gegliedertes hierarchisches System von Zertifizierungsinstanzen vor. An der Spitze steht eine sogenannte "Internet Policy Registration Authority (IPRA)". Die IPRA zertifiziert nur die unter ihr angesiedelten "Policy Certification Authorities (PCA)". Die PCAs zertifizieren weitere "Certification Authoriethies (CA)", und erst diese CAs zierti-fizieren Benutzer.

Die Idee von PEM ist es, Namenshierarchien mit Zertifizierungshierarchien in Verbindung zu bringen. Im Prinzip kann jeder Namensgeber gleichzeitig Zertifizierungsinstanz (CA) für die öffentlichen Schlüssel aller derjenigen Personen und Institutionen sein, denen er Namen verleiht. Davon ausgenommen sind lediglich die PCAs und die oberste IPRA. Man geht aber heute realistischerweise davon aus, dass es zwar viele PCAs und von ihnen zertifizierte CAs geben wird, nicht aber eine weltweit einzige IPRA, da andere Länder kaum akzeptieren würden, sich bei der kryptographischen Zertifizierung den Regeln einer höchsten Internet-Autorität, womöglich unter amerikanischer Dominanz, zu unterwerfen[72]. Realistischerweise geht man daher von einer Menge von PCAs aus, die sich gegenseitig quer-zertifizieren.

Die oberste Zertifizierungsstelle im deutschen Rechtsbereich ist

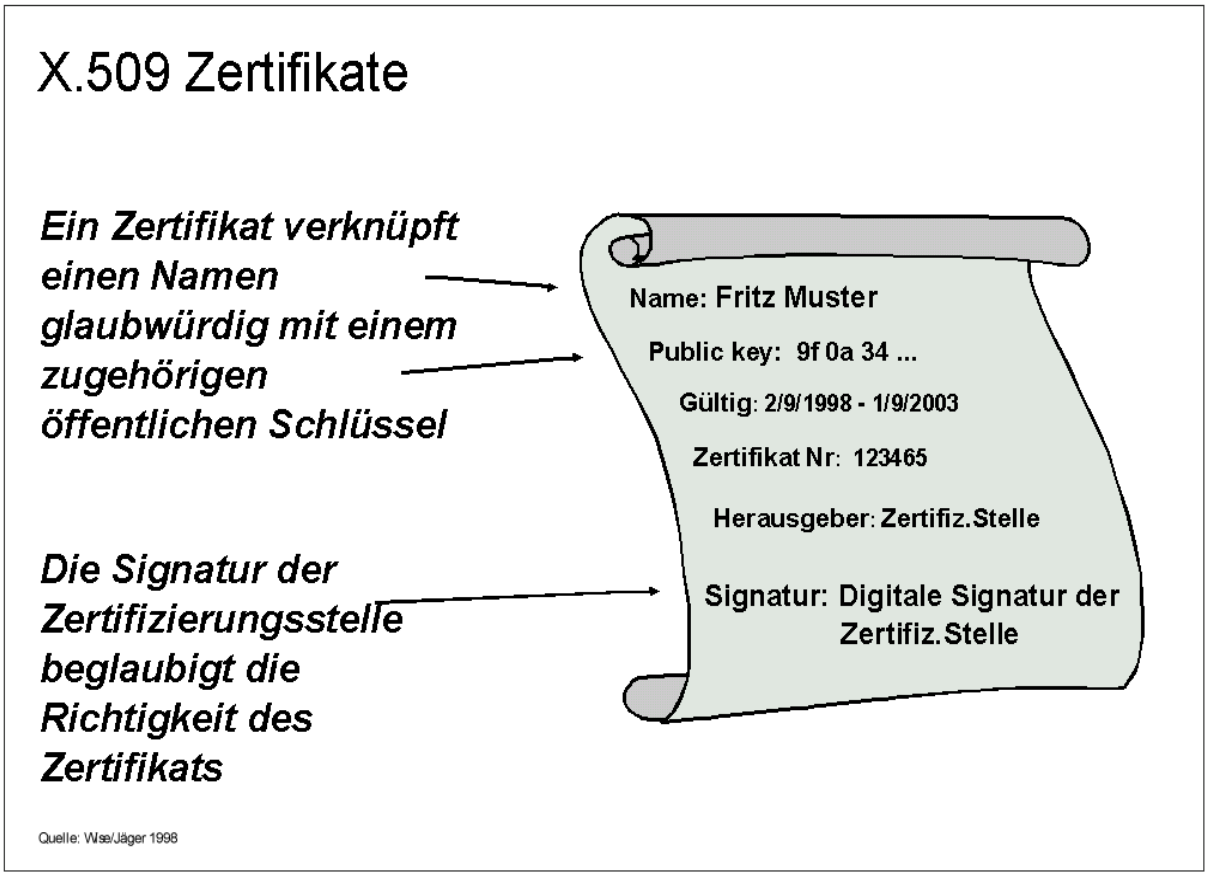
71Grimm, DuD 1996, 27, 31 f. m.w.N.; vgl. auch Schäfer, 1997, S. 89 ff.
72Grimm, DuD 1996, 27, 32

eine behördliche Instanz: Sei heißt kurz "Wurzel" und wird zur Zeit bei der Regulierungsbehörde für Telekommunikation und Post (Reg TP) in Mainz eingerichtet[73]. Die "Wurzel" zertifiziert alle logisch untergeordneten Zertifizierungsstellen im privaten Bereich. Auf diese Weise wird ein nationales deutsches Vertrauensnetz für Zertifikate eingerichtet. International kann das Vertrauensnetz erweitert werden, wenn die Nationen ihre eigenen "Wurzeln" gegeneinander anerkennen (engl. "cross certification")[74]. So kann ein globales Vertrauensnetz für das Internet entstehen.

Ein Zertifikat im Sinne des Signaturgesetzes ist gem. § 2 Abs. 3 SigG eine mit einer digitalen Signatur verstehene digitale Bescheinigung über die Zuordnung eines öffentlichen Signaturschlüssels zu einer natürlichen Person (Signaturschlüssel-Zertifikat) oder eine gesonderte digitale Bescheinigung, die unter eindeutiger Bezugnahme auf ein Signaturschlüssel-Zertifikat weitere Angaben enthält (Attribut-Zertifikat).

73Jäger, COMPUTERWOCHE Nr. 42 vom 16.10.1998; siehe auch §§ 2 Abs. 2, 14 Abs. 4 SigG
74Wise/Jäger, 1998, S. 12

Die relevanten Formate und Protokolle für die Automatisierung des Zertifizierungsvorgangs folgen dem X.509 Standard:



Der Vorteil einer derartig rigiden Zertifizierungsinfrastruktur liegt in der Glaubwürdigkeit der Zertifizierung, die auf einer transparenten Festlegung genauer Zertifzierungsregeln beruht. Vorbild bilden etwa das weltweit etablierte Ausweissystem mit Personalausweisen, Pässen, Mitarbeiterausweisen usw. Im Prinzip kann ein Beamter jedes Landes einen Ausweis eines anderen Landes verifizieren und damit eine Person authentifizieren, auch wenn

er ihr noch nie zuvor begegnet ist. Analog soll es auch im Internet sein[75]: Durch die Überprüfung eines Zertifikats kann jeder Benutzer jeden anderen Benutzer authentifizieren, auch wenn er ihm noch nie vorher begegnet ist. Damit ist z. B. ein weltweit offener Markt von spontanen und vertrauenswürdigen Behördenbeziehungen möglich.

Der Nachteil des Zertifizierungsmodells von PEM besteht darin, dass erst eine wirkungsvolle Infrastruktur von Zertifizierungsinstanzen aufgebaut werden muss, bevor Signatur- und Verschlüsselungsfunktionen sinnvoll angewendet werden können. Die Implementierung und schließlich der reale Betrieb von Zertifizierungsinstanzen sind aber schwierig, aufwendig und teuer.

Eine andere Kritik, die aus den Reihen der Bürger zu hören ist, argwöhnt, dass staatliche Stellen die Herrschaft über das Zertifizierungsgeschäft übernehmen und dadurch den Bürger auch mit krytographischen Mitteln überwachen könnten.

(2)*PGP-Verfahren*

In den vergangenen Jahren hat Phil Zimmermann mit einem frei verfügbaren Softwarepaket für digitale Signatur und Verschlüsselung mit RSA und IDEA, das er "Pretty Good Privacy (PGP)" genannt hat, viel Aufmerksamkeit erregt[76]. Die Besonderheit von PGP, die entscheidend zu seiner raschen Verbreitung beigetragen hat, ist sein einfaches Schlüsselverteilungsverfahren, das ohne eine Infrastruktur von Zertifizierungsinstanzen auskommt.

75Grimm, DuD 1996, 27, 33
76Grimm, DuD 1996, 27, 33 m.w.N.; vgl. auch Schäfer, 1997, S. 92 ff.

Freilich müssen bei PGP die öffentlichen Schlüssel genauso an ihre Benutzer gebunden werden, wie in jeder asymmetrischen kryptographischen Anwendung. Aber bei PGP überprüfen die Benutzer die öffentlichen Schlüssel ihrer Partner selbst[77]. Dadurch können Benutzer ganz spontan anfangen, öffentliche Schlüssel untereinander auszutauschen und dann gleich mit Verschlüsselung und digitalem Signieren miteinander beginnen.

Jeder PGP-Benutzer verfügt über eine eigene Sammlung öffentlicher Schlüssel, die PGP als "Public Key Ring" bezeichnet. Wenn man davon ausgeht, dass alle öffentlichen Schlüssel, die im Public Key Ring gespeichert sind, geprüft worden sind, kann man den Public Key Ring auch als Sammlung von "Zertifikaten" öffentlicher Schlüssel auffassen. Allerdings: Was steht in so einem "Zertifikat"? Nur ein öffentlicher Schlüssel und der Name des Schlüsselbesitzers. Bei vorsichtigem Umgang mit dem Prüfen und Weiterreichen von Schlüsseln wäre das Verfahren immer noch sicher. Allerdings verführt gegenseitige Prüfung zu einer gefährlichen Inflation des Schlüsselaustauschs. Personen tauschen nicht mehr nur einzelne Schlüssel, sondern gleich ihre ganzen Schlüsselsammlungen aus.

Wenn man nun über einen derart vollgeladenen Public Key Ring verfügt, welche Gewissheit geben einem dann noch die dort eingetragenen Bindungen zwischen öffentlichen Schlüsseln und zugehörigen Namen? Es gibt keinen Hinweis darauf, von wem und auf welche Weise diese Schlüssel jemals geprüft worden sind und ob sie überhaupt geprüft worden sind. Es ist ein Kinderspiel, gefälschte Namen in einen Public Key Ring einzuschleusen und so

77Grimm, DuD 1996, 27, 33

massenhaft unter die Leute zu bringen[78].

(3)*Stellungnahme*

Dadurch, dass das Zertifizierungsverfahren "PGP" nicht formalisiert ist und die Übernahme fremder "Zertifikate" nicht nachvollziehbar ist, eignet es sich nicht für die öffentliche Verwaltung. Das PEM-Modell erfordert erst den Aufbau einer Zertifizierungsinfrastuktur, bevor man die kryptographsichen Mechanismen sinnvoll anwenden kann.
Die beiden Modelle sind zwar verschieden, aber keineswegs unvereinbar. Im Gegenteil: PEM kann durch eine einfache Hinzunahme von Standardfunktionen den persönlichen bilateralen Austausch öffentlicher Schlüssel unterstützen. Das ist in dem Anwendungspaket SecuDE durch die sogannten "PKLists" (in der Rolle von Public Key Rings) und durch die "Fingerprint"-Funktion[79] bereits realisiert[80]. Umgekehrt kann das Zertifizierungsverfahren von PGP eine weitere Option für formalisierte Zertifizierungen hinzunehmen.
Bei einem abgestuften Sicherheitskonzept könnte man so auch in der öffentlichen Verwaltung mit dem Zertifizierungsprozess beginnen.

ee)**Zwischenergebnis**

Mit asymmetrischen Verschlüsselungsverfahren stehen also zwei

78Grimm, DuD 1996, 27, 34
79Vgl. dazu Grimm, DuD 1996, 27, 33 f.
80Grimm, DuD 1996, 27, 35 m.w.N.

Sicherheitsdienste zur Verfügung: zum einen die digitale Signatur, die die Authentizität der Kommunikationspartner, die Datenintegrität und die Nicht-Abstreitbarkeit des Ursprungs sicherstellt; und zum anderen die partnerbezogene Vertraulichkeit[81].

Mit Hilfe asymmetrischer Verschlüsselungsverfahren kann Sicherheit auch "nach außen", d. h. gegenüber neutralen Dritten (etwa einem Richter) gewährleistet werden. Denn die Benutzung eines geheimen Schlüssels ist bis auf seinen Besitzer rückführbar: niemand anders als er verfügt über ihn. Bei Verwendung von persönlichen Schlüsselpaaren wird deshalb die Sicherheit bis hin zu den Schlüsselbesitzern gewährleistet, und zwar auch über unsichere Netze hinweg, denn die Partner können durch geeignete Kodierung ihrer Daten Kryptogramme über beliebige Netze verschicken. Dadurch werden Telekooperationspartner auch über offene Netze geschäftsfähig.

Natürlich sind dabei hohe Sicherheitsanforderungen an die lokalen Systeme zu stellen. Zum Beispiel darf ein Besitzer seinen geheimen Schlüssel nicht verlieren oder "aus Versehen" außerhalb seiner Smartcard sichtbar machen können. Die lokalen Verschlüsselungsfunktionen müssen korrekt implementiert und unmanipulierbar sein. Die Bedienung muss so einfach und verständlich sein, dass dem Benutzer keine Fehler bei der Anwendung der Digitalen Signatur oder der Verschlüsselung unterlaufen können.

c)Hybridverfahren

81Grimm, DuD 1996, 27, 30

Digitale Signaturen und Kryptographische Anwendungen sind getrennt zu betrachten: Digitale Signaturen verwenden Kryptographie und sichere Anwendungen (z. B. für die Verschlüsselung von Dokumente, Schriftsätze) verwenden Kryptographie.

Für die Verbindung von Digitalen Signaturen und sicheren Anwendungen sind sogenannte "Hybridverfahren" modern geworden, bei denen die eigentliche Informationsverschlüsselung durch ein symmetrischen Verfahren und die Schlüsselverteilung asymmetrisch erfolgt, ein Ansatz, der in idealer Weise die Stärken symmetrischer und asymmetrischer Verfahren in sich vereinigt: die Schlüsselverteilung erfordert nicht länger den Kurier, während die Datenkryptierung in der geforderten Geschwindigkeit ablaufen kann[82].

Der zu verschlüsselnde (lange) Text wird mit einem schnellen symmetrischen Algorithmus verschlüsselt, und zwar mit einem symmetrischen Schlüssel, der extra für diesen einen Vorgang vom Sender erzeugt wird. Dieser (kurze) symmetrische Schlüssel wird nun mit einem asymmetrischen Verfahren verschlüsselt und so dem Kryptogramm des Textes beigefügt[83]. Das wird deshalb so gemacht, weil die bekannten asymmetrischen Verfahren, z. B. RSA oder ElGamal, bei langen Texten zeitaufwendig sind, während man sehr schnelle symmetrische Algorithmen kennt, z. B. DES oder IDEA, die genauso sicher sind. Das Hybridverfahren ist insgesamt ein asymmetrisches Verfahren, billiger als die reinen asymmetrischen

82Heuser, HMD 190/1996, 8, 11
83Grimm, DuD 1996, 27, 30

Verfahren, aber genauso sicher.

4. Sicherheit der Verschlüsselungstechnik

Jeder kryptographische Algorithmus kann, zumindest theoretisch, durch einen brute-force Angriff gebrochen werden[84]. Für ein Chiffrierverfahren kann man zum Beispiel den verwendeten geheimen Schlüssel mittels simplen Durchprobierens aller möglichen Schlüssel bestimmen, vorausgesetzt man verfügt über einen Klartextblock und dessen Verschlüsselung. Eine detaillierte Berechnung der Kosten für diese brute-force Attacke gegen DES ist 1994 von Wiener kalkuliert worden. Die Kosten für Entwicklung und Bau eines Spezialrechners, der in der Lage ist, alle möglichen DES Schlüssel in ungefähr 3,5 Stunden durchzuprobieren, betragen etwa eine Million US-Dollar[85].

Bei den asymetrischen Verfahren werden für die Verschlüsselung und für die Entschlüsselung verschiedene Schlüssel, ein öffentlich bekannter und ein geheimer, verwendet. Die beiden Schlüssel gehören zusammen und theoretisch kann aus dem einen Schlüssel der andere konstruiert werden[86]. In der Praxis ist jedoch der Aufwand so groß, dass dies in vertretbarer Zeit nicht möglich ist.

Die Fälschungssicherheit von RSA- und DSA-Signaturen beruht auf unbewiesenen, z. T. erst wenig untersuchten komplexitätstheoretischen Annahmen. Das bedeutet nicht, dass RSA und DSA unsicher sind, wohl aber, dass sie sich als unsicher erweisen

84Dobbertin, DuD 1997, 82, 83
85Dobbertin, DuD 1997, 82, 83; ähnlich auch Schäfer, 1997, S. 76
86Gerling, DuD 1997, 197, 198

könnten[87].

Im Sonderfall der Sicherung gespeicherter Daten durch RSA-Verschlüsselung tritt zu diesen Elementen noch dasjenige der Verlustsicherung hinzu: ein verloren gegangener oder zur Unzeit vernichteter Schlüssel könnte hier zum Datenverlust führen. Gefordert ist hier eine ordnungsgemäße Administrierung aller eingesetzter Schlüssel.

Dabei ist aber zu beachten, dass der mit dem Private-Key verschlüsselte Text nur mit dem Public-Key entschlüsselt werden kann und umgekehrt. Für den Fall, dass der Public-Key verloren gegangen ist, besteht die Möglichkeit, diesen bei der Zertifizierungsstelle zu erfragen. Mit diesem wäre sodann eine Entschlüsselung der eigenen Daten möglich.

Beim Verlust der Smartcard mit dem Private-Key entsteht nur das Problem, dass eine mit dem Public-Key verschlüsselte Nachricht zwar empfangen, aber nicht entschlüsselt werden kann. In einem solchen Fall müsste der Empfänger den Absender bitten, die Nachricht, verschlüsselt mit dem neuen Public-Key, erneut zu schicken[88].

Nach alledem besteht zwar ein Verlustrisiko, ein Schadensrisiko dürfte mit den vorherigen Ausführungen jedoch abzulehnen sein.

5. **Sicherheit der Smartcard selbst**

Nach Kruse/Peuckert[89] sind die im Chip gespeicherten Daten durch verschiedene Mechanismen geschützt. Eine Änderung sei nicht

87 Fox, DuD 1997, 69, 73
88 Vgl. dazu auch Pfitzmann, in: Hamm/Möller, 1998, S. 82
89 Kruse/Peuckert, DuD 1995, 142, 143

möglich.

Dem stehen jedoch die Untersuchungen von Kocar[90] und Wohlmacher/-Fox[91] gegenüber. Der Anwender sollte wissen, dass gewisse Manipulationen auf der Smartcard, wenn auch mit hohem Aufwand, möglich sind[92]. Der Hersteller sollte dann mit Gegenmaßnahmen die Mikrochipentwicklung vorantreiben. Nur einige Firmen haben ihre Mikrochips für Smartcards gegen solche direkten Angriffe aufgerüstet.

Neben einer Implementierung der benötigten Kryptoalgorithmen enthalten diese Smartcards alle erforderlichen geheimen Schlüssel des Benutzers. Damit hängt die Sicherheit der gesamten Anwendung maßgeblich von der Unausforschbarkeit des "Chips" ab[93].

Je nach Anforderungen an die Sicherheit der Anwendung, in der die Smartcard eingesetzt wird, muss überlegt werden, welche Schutzmechanismen zur Sicherheit des Chips eingesetzt werden müssen. Die Mehrkosten, die durch die Mechanismen entstehen, dürfen den Schaden nicht übersteigen, der ohne Schutzmechanismus durch erfolgreiche Angriffe verursacht werden könnte[94].

Die Angriffe auf Smartcards und ihre Algorithmen bedeuten allerdings nicht, dass Smartcards per se als Sicherheitstoken ungeeignet sind. Denn alle bekannt gewordenen Angriffe sind bereits durch geeignete Gegenmaßnahmen verhindert worden.

6. **Sicherheit bei Verlust der Smartcard**

90Kocar, DuD 1996, 421 ff.
91Wohlmacher/Fox, DuD 1997, 260 ff.
92Kocar, DuD 1996, 421, 423
93So auch Wohlmacher/Fox, DuD 1997, 260, 260
94Wohlmacher/Fox, DuD 1997, 260, 262

An vielen Automaten, Geräten und Computern ist mittlerweile die Eingabe einer PIN selbstverständlich geworden ist. Durch die damit verbundene starke Zunahme von PINs für die unterschiedlichsten Zwecke ist es für einen Normalbürger schon sehr schwierig geworden, den Überblick zu behalten. Wer kann sich aber schon 20 oder mehr verschiedene PINs merken? Auch ist es für die Sicherheit und den Ruf eines Systems naturgemäß ziemlich abträglich, wenn jeder Benutzer seine PIN auf der Karte notiert hat, da die Anzahl der Betrugsfälle zu groß wird[95].
Mit den vorherigen Ausführungen ist aber auch erkennbar, dass die Smartcard mit allen Methoden verwundbar ist, mit denen Passwörter angegriffen werden können: die unbefugte geheime Aufnahme der Nutzung mit einer Videokamera, das Ausprobieren von Geheimzahlen mit nachfolgender Sperre der Karte und dergleichen.
Empfehlenswert ist deshalb, andere Identifikationsverfahren als die PIN-Prüfung einzusetzen. Idial dafür sind sogenannte biometrische Merkmale, anhand derer eine Person von einer Maschine eindeutig identifiziert werden kann.

VI. ***Die Biometrie***

1. **Sinn und Zweck der Biometrie**[96]

Wie sich aus den vorherigen Ausführungen bereits ergibt, können die Identifikationsmittel des Nutzers verloren gehen, gestohlen

95Rankl/Effing, 3. Aufl. 1999, S. 451 f.
96Biometrie: Lehre von der Zählung und Körpermessung an Lebewesen

oder imitiert werden. Man kann zwar eine Smartcard stehlen und kommt gegebenenfalls hinter die PIN, niemand kann sich aber die Netzhaut, den Fingerabdruck oder das Sprachmuster eines anderen aneignen.

Außerdem garantieren diese traditionellen Identifikationsmittel lediglich, dass ein Benutzer zum entsprechenden Zeitpunkt im Besitz dieses Identifikationsmittels ist. Der berechtigte Besitz des jeweiligen Identifikationsmittels kann hingegen mit klassischen Methoden nicht überprüft werden.

Ein anschauliches Beispiel ist der Geldautomat um die Ecke. Wer die EC-Karte besitzt und die zugehörige PIN kennt, bekommt Geld. Wäre diese PIN-Autorisierung durch einen Fingerabdruckleser (Authentifizierung) ersetzt, könnte niemand mehr die Mutter oder den Sohn zum Automaten schicken. Allerdings kann auch kein Gangster mehr mit einer gefundenen und geknackten EC-Karte Geld abheben. Schließlich wird sich auch keiner, der unberechtigt Besitzer einer Smartcard eines Rechtsanwaltes geworden ist, Zugang zu dem Server eines Gerichts verschaffen können[97]. Neben dieser Unsicherheit wurde die unkomfortable Handhabung einer zunehmenden Anzahl von PINs (z. B. für Electronic Shopping und andere Online-Anwendungen) bereits zuvor dargestellt.

Hier bieten sogenannte biometrische Verfahren Lösungen, die sowohl die Ansprüche nach mehr Sicherheit als auch nach mehr Komfort befriedigen. Anstelle der Überprüfung von Wissen oder Besitz analysieren biometrische Verfahren Charakteristika der Person. Ein biometrisches Identifizierungsverfahren ist ein Verfahren, das auf der Grundlage von einzigartigen, individuellen

97Zu beachten ist, daß der JKomG-BReg, Seite 55, keine Regelungen über biometrische Verfahren enthält.

und biologischen Merkmalen eine Person eindeutig identifizieren kann[98].

Nach Daly[99] haben sich biometrische Sicherheitsgeräte schon seit 20 Jahren als absolut zuverlässige Wächter in wichtigen amerikanischen Dienststellen bewährt. Sie prüfen aufgrund von untrüglichen persönlichen Merkmalen die Legitimation von Personen, die Zugang haben wollen. Auch kommerzielle Institutionen und Unternehmen bedienen sich solcher Geräte in zunehmendem Maße. Es gibt dafür viele Gründe, nicht zuletzt die Tatsache, dass der Preis einiger dieser Sicherheitsgeräte in der letzten Zeit stark gefallen - von 9000 Dollar im Jahr 1985 auf weniger als 2000 Dollar heute[100].

Die heutzutage am meisten verwendeten biometrischen Sicherheitsgeräte sind Fingerabdruckleser, Retina-Scanner sowie Geräte zur Erkennung der Handgeometrie und der Unterschrift. Zur Neuaufnahme einer Person und zur Überprüfung von bereits Aufgenommenen wird dasselbe Gerät benutzt. Die vom Berechtigten abgenommene Erkennung wird später mit der Kennung der Zugang suchenden Person verglichen. In vielen Fällen wird die Person zusätzlich noch einen persönlichen Identifikationscode (PIN oder Passwort) eingeben, wobei beide Prüfungen übereinstimmen müssen, damit der Zugang gewährleistet wird[101].

Zur Identifizierung einer Person eignen sich natürlich nicht alle biologischen Merkmale. Die folgenden Punkte müssen zu-

98Rankl/Effing, 3. Aufl. 1999, S. 458; ähnlich auch Wirtz, DuD 1999, 129, 129
99Daly, COMPUTERWOCHE Nr. 50 vom 11.12.1992
100Daly, COMPUTERWOCHE Nr. 50 vom 11.12.1992
101Daly, COMPUTERWOCHE Nr. 50 vom 11.12.1992

mindest erfüllt sein, damit sich ein Merkmal auch sinnvoll nutzen lässt[102]:

-Das Merkmal muss technisch gut messbar sein (Messmethode, Messdauer, Messkosten).

-Das Merkmal muss eindeutig einer bestimmten Person zuzuordnen sein.

-Eine Veränderung des Merkmals in betrügerischer Absicht darf nicht möglich sein.

-Die erzeugten Referenzdaten müssen klein sein (maximal wenige hundert Bytes).

-Die natürlichen Veränderungen des Merkmals über die Zeit müssen so gering sein, dass das Merkmal immer einwandfrei messbar bleibt.

-Die Messmethode und das Merkmal müssen von den Benutzern akzeptiert werden.

2.**Biometrische Systeme**

Bei den biometrischen Identifizierungsverfahren unterscheidet man zwischen physiologischen und verhaltensbasierten Merkmalen[103]. Letztere sind direkt mit dem Körper einer Person verbunden und sind von bewussten Verhaltensmustern unabhängig. Bei dem verhaltensbasierten biometrischen Verfahren sind die Merkmale innerhalb gewisser Grenzen veränderbar. Im folgenden werden die wesentlichen und am häufigsten verwendeten biometrischen Merkmale dargestellt.

102Rankl/Effing, 3. Aufl. 1999, S. 460
103Vgl. dazu Rankl/Effing, 3. Aufl. 1999, S. 458 ff.

a)Physiologische Merkmale

Die nicht bewusst änderbaren physiologischen Merkmale unterliegen im Laufe der Zeit nur geringen Veränderungen. So ändern sich beispielsweise die charakteristischen Muster von Fingerabdrücken im gesamten Leben nie.

aa)**Gesicht**

Als biometrisches Merkmal eignet sich zunächst das menschliche Gesicht. Die Umsetzung dieser Erkenntnis in die technische Realisierung ist aber mit vielen Tücken verbunden. Gesichter können sich innerhalb kurzer Zeit stark verändern, und ihr Aussehen hängt sehr stark von äußeren Umständen ab[104]. Man denke nur an Brille, Bart, Make-up, Beleuchtung oder Aufnahmewinkel des Gesichts.

bb)**Retina**

Die Retina (Netzhaut) des menschlichen Auges ist aufgrund ihrer Knoten und Verzweigungen der Blutbahnen für jede Person unterschiedlich. Abgetastet wird mit einem die Pupille durchdringenden Lichtstrahl im infraroten Wellenlängenbereich[105]. Da man zur Identifizierung seine Augen sehr nahe an das Abtastgerät heranbringen muss, stößt allerdings das Verfahren bei den

104Rankl/Effing, 3. Aufl. 1999, S. 463
105Rankl/Effing, 3. Aufl. 1999, S. 464

Benutzern überwiegend auf Ablehnung. Ein weiteres Problem sind bestimmte Arten von Kontaktlinsen. Diese schirmen Wellenlängenbereiche im infraroten Bereich stark ab, wodurch die Messung in der Regel versagt.

cc)**Iris**

Die Iris (Regenbogenhaut) begrenzt als variable Lochblende den Strahlengang zur Netzhaut. Sie ist ein biologisches Merkmal, das ähnlich wie die Netzhaut für eine bestimmte Person eindeutig ist[106]. Bei der Abtastung der Iris kann mehr Abstand von dem Messgerät gehalten werden als bei der Prüfung der Netzhaut, da das Messverfahren einfacher ist. Aber auch hier können Probleme durch Kontaktlinsen auftreten, die die Messung unter Umständen stark beeinflussen.

dd)**Geometrie der Hand**

Schon seit den 70er Jahren werden Identifikationssysteme eingesetzt, die auf der Grundlage einer dreidimensionalen Vermessung der Hand oder Teilen davon arbeiten[107]. Als Ausgangspunkt der Messungen können beispielsweise Fingerlänge, Fingerdurchmesser und Radius der Fingerkuppen verwendet werden[108]. Da nur wenige Abtastpunkte für eine Identifizierung genügen, ist das Verfahren auch hinreichend schnell und für den Benutzer unkompliziert. Er legt einfach seine Hand in ein Gerät, und

106Rankl/Effing, 3. Aufl. 1999, S. 464
107Rankl/Effing, 3. Aufl. 1999, S. 464
108Rankl/Effing, 3. Aufl. 1999, S. 464

dieses nimmt die Messung vor.

ee)**Fingerabdruck**

Das bekannteste auf physiologischen Grundlagen beruhende biometrische Verfahren ist die Identifizierung mittels Fingerabdruck. Der Daumen oder auch eine andere Fingerkuppe wird auf eine durchsichtige Platte gelegt, und eine darunter angebrachte Kamera tastet die Hautoberfläche berührungslos ab[109]. Viele Systeme besitzen zusätzlich zur optischen Abtasteinheit Sensoren zur Messung von Temperatur oder des Pulses im Finger. Damit soll sichergestellt werden, dass keine von der Hand abgetrennten Finger zur Identifizierung verwendet werden können. Allerdings konnten Anfang 2007 Einbrecher in Rom das (wohl veraltete) Sicherheitssystem einer Bankfilia1e überlisten, indem sie den amputierten Finger einer Frauenleiche zum Einsatz brachten[110].
In manchen Benutzerkreisen gibt es eine Abneigung gegen dieses Verfahren, da es bekanntermaßen seit vielen Jahren in der Verbrechensbekämpfung eingesetzt wird. Problematisch können auch kleinere Verletzungen an den Fingerkuppen für die einwandfreie Personenidentifizierung sein. Trotzdem sind Fingerabdruck-Systeme sehr weit verbreitet, da sie vom technischen Aufwand und von der Benutzerakzeptanz verhältnismäßig problemlos sind.

b)Verhaltensbasierte Merkmale

109Rankl/Effing, 3. Aufl. 1999, S. 465
110FAZ, 29.01.2007, S. 9

Verhaltensbasierte biometrische Merkmale bleiben über die Zeit hinweg bei vielen Personen nicht stabil. Dies wird besonders deutlich bei der Unterschrift, die im Laufe des Lebens starken Veränderungen unterworfen ist. Diese Veränderungen treten aber in den seltensten Fällen schlagartig auf, sondern ganz allmählich und langsam. Deshalb benutzen viele Systeme hier adaptive Verfahren, die festgestellte Veränderungen an dem biometrischen Merkmal bei korrekter Identifikation dann als neues Refernzmuster übernehmen und in der Smartcard speichern[111].

aa)**Schreibrhythmus**

Untersuchungen haben ergeben, dass es beim Eintippen von Zeichen auf einer Tastatur sehr große Unterschiede zwischen einzelnen Personen gibt[112]. Dies kann natürlich als biometrisches Merkmal zur Identifizierung benutzt werden. Der große Vorteil des Verfahrens ist, dass keine zusätzliche Hardware benötigt wird, da eine Tastatur und ein Computer in den meisten Fällen ohnehin bereitsteht. Leider werden bei diesem Verfahren zwischen 100 und 150 alphanumerische Zeichen benötigt, welche noch dazu im Zehnfingersystem eingetippt werden müssen, um eine Person sicher zu erkennen. Dies ist ein besonders großer Nachteil des Verfahrens.

bb)**Stimme**

111Rankl/Effing, 3. Aufl. 1999, S. 466
112Rankl/Effing, 3. Aufl. 1999, S. 466

Ähnlich wie das Gesicht ist auch die Stimme für einen bestimmten Menschen charakteristisch. Das dafür vorgesehene biometrische Verfahren ist nicht ohne Nachteile. Die Stimme eines Menschen ist sehr stark von seiner aktuellen körperlichen Verfassung abhängig[113]. Auch müssen bei einer Stimmerkennung zuverlässig alle Hintergrundgeräusche ausgeblendet werden, um überhaupt eine eindeutige Spektralanalyse durchführen zu können. Um Angriffe durch Wiedereinspielung zu verhindern, muss bei jeder Identifikation ein anderer Satz aufgesagt werden, was das Verfahren sehr erschwert und die Erkennung aufwendig macht. Diesen technischen Schwierigkeiten steht allerdings eine gute Benutzerakzeptanz gegenüber, was diese Methode der biometrischen Benutzeridentifikation durchaus interessant macht.

cc)**Dynamische Unterschrift**

Die einzige im täglichen Umgang gewohnte Identifizierungsmethode ist die Leistung einer Unterschrift. Sie kann aufgrund des sehr individuellen Charakters ebenfalls als biometrisches Merkmal verwendet werden[114]. Da die Unterschrift im täglichen Gebrauch von jedem verwendet wird, hat sie zur Identifizierung einer Person die höchste Akzeptanz aller Verfahren. Aber auch hier sind die technischen Lösungen nicht einfach, da sich die Unterschrift mit der Zeit ändert und nie völlig gleich ist.

3.**Stellungnahme**

113Rankl/Effing, 3. Aufl. 1999, S. 466 f.
114Rankl/Effing, 3. Aufl. 1999, S. 467

Bereits seit 1997 bemüht sich die UN-Luftfahrtorganisation ICAO im internationalen Rahmen um die Einführung maschinenlesbarer Ausweise mit biometrischen Informationen zur Erhöhung der Sicherheit im Flugverkehr. Die Terrorangriffe vom 11. September 2001 beschleunigten diese Arbeiten. Bis Ende dieses Jahres wird die EU ein internationl abgestimmtes System für Pässe mit biometrischen Merkmalen verabschieden, das Anfang 2006 in der Bundesrepublik eingeführt werden soll[115]. Damit wird deutlich, dass Sicherheit und Datenschutz eine besondere Bedeutung im Verhältnis Bürger - Verwaltung haben. Von diesem Standpunkt aus betrachtet scheint der Einsatz von Smartcards mit biometrischen Identifizierungsverfahren unvermeidbar und zwingend zu sein. Menschliche Schwächen, wie z. B. das leichtfertige Aufschreiben der PIN oder das Verleihen der Karte samt PIN, würden entfallen. Ein möglicher Dieb benötigt für einen Datenzugriff zusätzlich den Fingerabdruck oder die Stimme, ggf. sogar beides in Verbindung.
Die Vergabe einer PIN scheint m. E. aber auch weiterhin sinnvoll zu sein. Bei einem Raubüberfall muss der Karteninhaber dem Täter zusätzlich die PIN mitteilen. Das Vorhalten eines künstlichen oder abgehackten Gliedes reicht damit nicht aus. Dies steigert die Sicherheit des Bürgers.
Außerdem ist die Eingabe der PIN nicht nur für die Überprüfung, ob der Benutzer ein Geheimnis kennt, notwendig, sondern auch für die juristische Willensbekundung "ich bin einverstanden"[116].

115Schiffhauer, FAZ vom 01.06.2004, Seite T 1
116So auch Rankl/Effing, 3. Aufl. 1999, S. 459

Dieser Zusammenhang ist sehr wichtig, wenn man andere Verfahren als die PIN-Prüfung verwenden will. Eine Willensbekundung eines Benutzers wird m. E. wohl abzulehnen sein, wenn sein Augenhintergrund aus drei Metern Entfernung überprüft wird. In fast allen Ländern muss daher der Benutzer bewusst etwas manuell ausführen, damit dies als Willensbekundung ausgelegt werden kann. Nach Donnerhacke[117] sei ferner noch einige Forschungsarbeit zu leisten, bis ein Fingerscanner wirklich nur auf lebende Finger reagiert und nicht auf abgehackte Stücke. Dazu dient bereits aber die Lebenderkennung: Unter Lebenderkennung wird die Überprüfung verstanden, ob die jeweiligen biometrischen Merkmale auch von einem lebenden Organismus und nicht von einer künstlichen Fälschung erzeugt wurden[118]. Bei einigen Biometrien muss hier zwar explizit Vorsorge getragen werden, da diese eine künstliche Fälschung - durch Verwendung eines Kunstfingers bei optischen Fingerabdruckssystemen, eines Bildes oder Videos bei Gesichtserkennungssystemen, einer Sprachaufnahme bei Sprechverifikationssystemen - nahelegen[119]. Überwiegend kann dieses Problem aber m. E. auf einfache Weise algorithmisch gelöst werden (z. B. gemeinsame Sprach- und Gesichtserkennung), während bei anderen wie der Fingerabdruckserkennung mit Wärmesensoren explizite Vorsorge getroffen werden muss. Nach Wirtz[120] werden hier mit der Zeit multiple biometrische Verfahren eine Abhilfe schaffen, die durch die Kombination lebenderkennungsbedürftiger Techniken mit solchen, die eine Lebenderkennung implizit vollziehen [z. B.

117Donnerhacke, DuD 1999, 151, 154
118Wirtz, DuD 1999, 129, 130
119Wirtz, DuD 1999, 129, 130
120Wirtz, DuD 1999, 129, 131

Pulsmessung im Finger], Sicherheit und Komfort für den Endnutzer erhöhen. Ferner könnte der Schutz des Nutzers m. E. auch dadurch erhöht werden, indem mehrere Finger in einer bestimmten Reihenfolge auf den Sensor gelegt werden müssen. In diese Richtung scheinen auch die Vorgaben der ICAO zu gehen: Danach werden die Abdrücke von mindestens zwei Fingern europäischer Standard sein[121].

VII. ***Schlussbemerkungen***

Zu den bemerkenswertesten Vorteilen der Smartcard gehört ihre Multifunktionalität. Da Smartcards ohnehin initialisiert und personalisiert werden müssen, besteht die Möglichkeit, persönliche Daten auf die Karten sichtbar aufzubringen und elektronische persönliche Daten auf den Chips abzuspeichern. Auch Zertifikate und private Schlüssel werden während der Personalisierung auf die Smartcard gebracht. Die Smartcard für den Netzwerk-Zugang kann damit auch in der öffentlichen Verwaltung als Mitarbeiterausweis mit Passfoto benutzt werden. Weitere Daten für elektronische Geldbörsenfunktion, Gleitzeit-Erfassung, Zutritt zu Sicherheitszonen können zusätzlich auf die Smartcard geladen werden[122]. Die Integration mehrerer Anwendungen dämmt den Anstieg der Kartenflut, spart Kosten und vereinfacht die Benutzung für den Karteninhaber[123]. Es bleibt zu hoffen, dass der zukünftige EU-Ausweis diese Fähigkeiten besitzen wird.
Das Ziel einer Anwendung muss schließlich sein, eine abgestufte

121Schiffhauer, FAZ vom 01.06.2004, Seite T 1
122Wise/Jäger, 1998, S. 20
123Kruse/Peuckert, DuD 1995, 142, 143 f.

Zugangskontrolle für verschiedene Räume und Rechnersysteme auf der Grundlage von Smartcards zu schaffen[124]. Es befinden sich also an bestimmten Türen und Rechnern Terminals, die die entsprechenden Türen oder Rechner nach einer Kommunikation mit einer Karte freischalten können. Dabei ist es wichtig, dass die Möglichkeit vorhanden ist, Sicherheitsniveaus zu definieren, zu denen nur ein bestimmter Personenkreis Zugang erlangen darf. Der Zugang wird auf der Grundlage einer Authentisierung und eines Identitätsnachweises des Benutzers gewährt. Dieser Nachweis wird zum einen durch den Besitz der Smartcard und zum anderen durch die Kenntnis der dazugehörigen PIN - und noch besser durch wenigstens ein biometrisches Merkmal - geführt. Zur Überprüfung des rechtmäßigen Karteninhabers könnten sogenannte "Sensor-on-Card"-Lösungen zur Anwendung kommen, bei denen ein Fingerabdrucksensor direkt auf der Karte implantiert wird. Stimmt der Fingerabdruck und die PIN mit den Daten auf der Smartcard überein, so ist ein Zugang erlaubt. Die Terminals müssen einfache Sperrlisten führen können, um den Zugang durch "verlorene" Karten zu verhindern und um diese Karten dann gegebenenfalls irreversibel zu sperren.

Durch den Einsatz der Smartcard lässt sich das sogenannte "Hacker-Problem" wirkungsvoll verhindern. Hacker haben keinen Erfolg mehr damit, Passwörter mit Routinen auszuprobieren, Leitungen abzuhören oder in Passwortdateien einzudringen. Ein Zugang ohne Smartcard und ohne eine erfolgreiche Authentifikation nach dem Challenge-Response-Verfahren ist dann unmöglich.

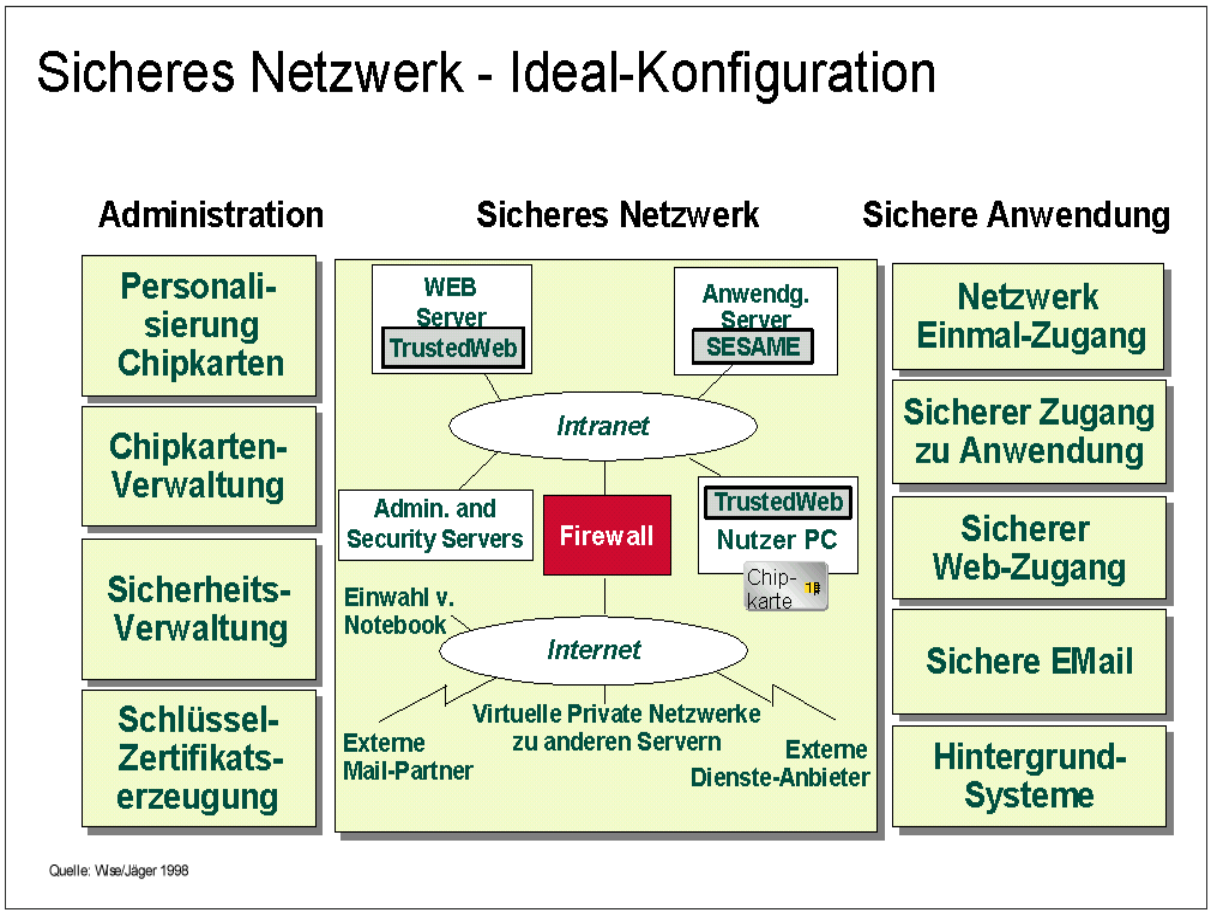
Die Sicherungsmaßnahmen müssen sich am Wert der zu schützenden

124Konkretes Beispiel bei Rankl/Effing, 3. Aufl. 1999, S. 732 ff.

Information orientieren. Die Entscheidung für eine der vielfältigen Möglichkeiten der Verifizierungsverfahren bedingt immer eine Abwägung des finanziellen und personellen Aufwands gegenüber dem Nutzen, dem durch die Sicherungsmaßnahme erreichbaren Schutz und dem verbleibenden Restrisiko[125]. Ist ein besonders hohes Sicherheitsniveau notwendig, sollte die Authentifikation über eindeutige Personenmerkmale (Biometrie) erfolgen. Die sichere Authentifikation erreicht dadurch ein außerordentlich hohes Niveau und ist durch den Einsatz der Smartcard praktikabel, weil die Referenzdaten weder in einer Datei gespeichert, noch online abgefragt werden müssen[126]. Sensitive Räume (mit Applikationen) sind auch weiterhin durch einen Schließmechanismus zu schützen. Aber auch vor verärgerten Angestellten, die es verstehen, in für sie sonst unzufriedene Informationssysteme einzudringen, schützt die Smartcard mit biologischen Merkmalen.

125Kiefer, HMD 190/1996, 48, 60
126Kruse/Peuckert, DuD 1995, 142, 145

Die folgende Abbildung stellt eine Idealkonfiguration eines sicheren Netzwerkes dar:



Abschließend sei auf folgendes - bei allen Lebensverhältnissen immanentes - Restrisiko hingewiesen: "Es bleibt die sichere Erkenntnis, dass nichts so unsicher ist wie die Sicherheit - nur eines ist sicher: dass es keine Sicherheit gibt."[127]

127Kersten, HMD 190/1996, 5, 6

Literaturverzeichnis:

Björk, Karl, Alles auf eine Karte gesetzt. Smart Cards und digitale Signaturen räumen Sicherheitsrisiken aus dem Weg, FAZ, E-Commerce-Beilage vom 01.06.1999, Seite B 16

Borking, John, **Verhaar**, Paul, Biometrie und Datenschutz, DuD 1999, 138

Daly, James, Biometrische Verfahren der Benutzeridentifikation, COMPUTERWOCHE Nr. 50 vom 11.12.1992

Dobbertin, Hans, Digitale Fingerabdrücke, DuD 1997, 82

Donnerhacke, Lutz, Anonyme Biometrie, DuD 1999, 151

Fox, Dirk, Fälschungssicherheit digitaler Signaturen, DuD 1997, 69

Gerling, Rainer W., Verschlüsselungsverfahren, DuD 1997, 197

Grimm, Rüdiger, Kryptoverfahren und Zertifizierungsinstanzen, DuD 1996, 27

Gundermann, Lukas, **Köhntopp**, Marit, Biometrie zwischen Bond und Big Brother, DuD 1999, 143

Hamm, Rainer, **Möller**, Klaus Peter, (Hrsg.), Datenschutz durch Kryptographie: ein Sicherheitsrisiko? Baden-Baden 1998 (zitiert: Bearbeiter, in: Hamm/Möller, 1998)

Heuser, Ansgar, Kryptographie: der Schlüssel zu mehr Datensicherheit in der Informationstechnik, HMD[128] 190/1996, 8

Heuser, Ansgar, Verschlüsselung in der öffentlichen Verwaltung, DuD 1996, 659

Jäger, Helmut, Chipkarten mit Koprozessor sollen E-Commerce absichern - Technik und Recht müssen Hand in Hand gehen, COMPUTERWOCHE Nr. 42 vom 16.10.1998

Jäger, Helmut, Netzsicherheit mittels Smart Cards für mittelständische Unternehmen, Siemens AG (Hrsg.) München 1999 (zitiert: Jäger, NETZSICHERHEIT 1999)

Jäger, Helmut, Neue Anwendungsmöglichkeiten für Chipkarten (zitiert: Jäger, 1997)

Jäger, Helmut, SINACARD - Chipkartenunterstütztes Sicherheitssystem für Firmennetzwerke, Siemens AG (Hrsg.) München 1999 (zitiert: Jäger, SINACARD 1999)

Justizkommunikationsgesetz: Gesetzesentwurf der Bundesregierung eines Gesetzes über die Verwendung elektronischer

128Führt ab Heft 150 den Untertitel "Theorie und Praxis der Wirtschaftsinformatik".

Kommunikationsformen in der Justiz (Justizkommunikationsgesetz - JKomG) vom 28.07.2004 (zitiert: JKomG-BReg)

Kiefer, Erich, Informationssicherung: Verfahren zur Nutzungskontrolle von EDV-Ressourcen, Kryptographie, Chipkarten, HMD 190/1996, 48

Kocar, Osman, Hardwaresicherheit von Mikrochips in Chipkarten, DuD 1996, 421

Kockskämper, Sabine, Für eine Sicherheit ist jeder selbst verantwortlich. Sicher elektronische Kommunikation braucht Authentizität, Integrität und Vertraulichkeit, FAZ, E-Commerce-Beilage vom 01.06.1999, Seite B 16

Kowalski, Bernd, Telesec - Verfahren zur Telesicherheit der Deutschen Telekom AG 190/1996, 75

Kruse, Dietrich, **Peuckert**, Heribert, Chipkarte und Sicherheit, DuD 1995, 142

Münzenberger, M., Public-Key-Kryptosysteme, HMD 190/1996, 31

Munzert, Michael, **Wolff**, Christian, Firewalls - Schutz vor Angriffen aus dem Internet, DuD 1996, 89

Rankl, Wolfgang, **Effing**, Wolfgang, Handbuch der Chipkarten: Aufbau - Funktionsweise - Einsatz von Smart-Cards, 3. Aufl.,

München, Wien 1999 (zitiert: Rankl/Effing, 3. Aufl. 1999)

Reiser, Christian, Internet - die Sicherheitsfragen: Antworten für Manager und Techniker, Wien 1998 (zitiert: Reiser, 1998)

Schäfer, Georg, Mit Sicherheit erfolgreich: ein Leitfaden zur Sicherung moderner Informations- und Kommunikationssysteme, Heidelberg 1997 (zitiert: Schäfer, 1997)

Schiffhauer, Nils, Der Bauer erkennt seine Tiere am Gang. Beim Menschen orientiert man sich an Gesicht, Fingern und Iris / 2006 kommen Pässe mit biometrischen Merkmalen, FAZ vom 01.06.2004, Seite T 1

Schmidt, Holger, Gezielte Angriffe von Computer-Hackern schrecken die Unternehmen auf. Sicherheitsbewusstsein steigt / Hacker kommen meist aus Amerika und Asien / "Script-Kiddies" auf dem Vormarsch, FAZ vom 11.02.2002, Seite 24

Stollenmayer, Peter, Sicherheitsdienste und Mechanismen in der Telekommunikation, HMD 190/1996, 61

Volpe, Francesco P., **Volpe**, Safinaz, Chipkarten: Grundlagen, Technik, Anwendungen, Hannover 1996 (zitiert: Volpe/Volpe, 1996)

Weck, Gerhard, Sicherheit von Client/Server-Systemen, DuD 1995, 224

Wirtz, Brigitte, Biometrische Verfahren, DuD 1999, 129

Wise, Andrew, **Jäger**, Helmut, Netzwerksicherheit und Chipkarte, Siemens Nixdorf AG (Hrsg.), München 1998 (zitiert: Wise/Jäger, 1998)

Wohlmacher, Petra, **Fox**, Dirk, Hardwaresicherheit von Smartcards, DuD 1997, 260