ARBEITSPAPIERE

aus der Begleitforschung zum Städtewettbewerb Multimedia *MEDIA*@Komm

2/2000

MEDIA @Komm

Ausgangssituation, Rahmenbedingungen und Hintergründe für die Umsetzung der *MEDIA*@Komm-Projekte

Begleitforschung *MEDIA*@Komm

Stand: Mai 2000

Autoren: Hermann Behrens, Martin Eifert, Holger Floeting, Busso Grabow, Roland Krüger, Lutz Schreiber, Arnold Schulz, Christine Siegfried, Claudia Stapel-Schulz, Hermann Strack

Herausgeber: Deutsches Institut für Urbanistik

Impressum

Autorinnen und Autoren

Dipl.-Geogr. Holger Floeting (Difu)
Dr. rer. pol. Busso Grabow (Difu)
Dipl.-Pol. Christine Siegfried (Difu)

Arnold Schulz (DIN)

Martin Eifert (HBI)
Lutz Schreiber (HBI)
Claudia Stapel-Schulz (HBI)

Roland Krüger (TÜViT)
Hermann Strack (TÜViT)
Berthold Weghaus (TÜViT)

Redaktion

Klaus-Dieter Beißwenger

Textverarbeitung und Layout

Christina Blödorn
Elke Postler

Deutsches Institut für Urbanistik
Straße des 17. Juni 110
10623 Berlin

Telefon: (030) 39001-0
Telefax: (030) 39001-100
E-Mail: difu@difu.de
Internet: http://www.difu.de

Schutzgebühr DM 20,–

Berlin, November 2000

Inhalt

1. Digitale Signatur (digSig) 5

1.1 Rechtliche Rahmenbedingungen für digitale Signaturen [Autoren: Martin Eifert, Lutz Schreiber, Claudia Stapel-Schulz (HBI)] 5

1.2 Digitale Signatur – technische Voraussetzungen und Probleme [Autor: Hermann Strack (TÜViT)] 8

1.2.1 Einführung 8

1.2.2 Verschlüsselung 9

1.2.3 Digitale Signaturen und Public-Key-Infrastruktur (PKI) 10

1.2.4 Funktionsweise digitaler Signaturen 11

1.2.5 Technische Voraussetzungen und Probleme 12

1.3 Ökonomische Fragen bei der Verbreitung der digitalen Signatur [Autor: Busso Grabow (Difu)] 16

2. Online-Dienstleistungen der Verwaltung unter Nutzung der digitalen Signatur .. 20

2.1 Verwaltungsmodernisierung [Autorin: Christine Siegfried (difu)] 20

2.1.1 Binnenperspektive: Effizienzsteigerung des Verwaltungshandelns 21

2.1.2 Außenperspektive des IuK-Einsatzes in Verwaltungen 24

2.2 Restriktionen bei der Gestaltung der interaktiven Verwaltung [Autorin: Christine Siegfried (Difu)] 27

2.3 Rechtliche Voraussetzungen [Autoren: Martin Eifert, Lutz Schreiber, Claudia Stapel-Schulz (HBI)] 29

2.4 Technische und sicherheitstechnische Voraussetzungen und Probleme [Autor: Roland Krüger (TÜViT)] 30

2.4.1 Einführung 30

2.4.2 Sicherheitskonzept für IT-Systeme 33

2.4.3 Exkurs: Einführung in den IT-Grundschutz 35

2.4.4 Anforderungen an technische Komponenten für Online-Dienstleistungen der Verwaltung unter Nutzung der digitalen Signatur 39

2.5 Ökonomische Voraussetzungen und Fragen [Autor: Busso Grabow (Difu)] 48

2.5.1 Individuelle Nutzenerwägungen – mikroökonomische Sicht 48

2.5.2 Volkswirtschaftlicher Nutzen – makroökonomische Sicht 50

3. E-Commerce und E-Payment 52

3.1 E-Commerce-Diffusion [Autor: Holger Floeting (Difu)] 52

3.1.1 Business-to-Business 52

3.1.2 Business-to-Consumer 56

3.2 Elektronische Marktplätze [Autor: Holger Floeting (Difu)] 57

3.3 Electronic Payment [Autorin: Christine Siegfried (Difu)] 59
3.3.1 Elektronisches Bezahlen mit der EC-Karte: POS/POZ, ELV 59
3.3.2 Einkaufen im Internet mit Kreditkarte: SET und SSL 59
3.3.3 Elektronisches („virtuelles") Geld: ECash, CyberCash, Geldkarte .. 60
3.4 Rechtliche Aspekte von Electronic Commerce und Electronic Payment [Autoren: Martin Eifert, Lutz Schreiber, Claudia Stapel-Schulz (HBI)] 63
3.4.1 Die EU-Richtlinie zum Electronic Commerce 63
3.4.2 Fernabsatzrichtlinie 64
3.4.3 Elektronischer Zahlungsverkehr 64
3.5 Technische Voraussetzungen und Probleme [Autor: Berthold Weghaus (TÜViT)] 66
3.5.1 Anforderungen an elektronischen Wirtschaftsverkehr 66
3.5.2 Anforderungen an E-Commerce-Systeme 68
3.5.3 Klassifizierung der einsetzbaren Protokolle und Standards 74
4. Integration und Kooperation [Autor: Busso Grabow (Difu)] 96
4.1 Wechselwirkungen 96
4.2 Kooperation und Zusammenführung von Kompetenzen 100
4.3 Gemeinsame Plattformen für öffentliche Online-Services und E-Commerce 102
5. Stand der Normung zur IT-Sicherheit, digitalen Signatur und bei Identifikationskarten [Autor: Arnold Schulz (DIN)] 104
5.1 Normen für die IT-Sicherheit 106
5.2 Normen für Identifikationskarten 109
5.3 Normen für den elektronischen Geschäftsverkehr 111
5.4 CEN – Workshop – Agreements (CWA) 111

1. Digitale Signatur (digSig)

1.1 Rechtliche Rahmenbedingungen für digitale Signaturen [Autoren: Martin Eifert, Lutz Schreiber, Claudia Stapel-Schulz (HBI)]

Nachdem die Europäische Kommission den Mitgliedstaaten am 13. Mai 1998 ihren Vorschlag für eine „Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen“ (Sig-Ril) unterbreitete[1] und der Europäische Rat am 22. April 1999 einen gemeinsamen Standpunkt im Hinblick auf den Erlass der Richtlinie verabschiedete[2], wurde diese durch Beschluss des Rates vom 30. November 1999 angenommen und trat am 19. Januar 2000 in Kraft[3]. Die Mitgliedstaaten sind nun verpflichtet, sie innerhalb von 18 Monaten umzusetzen. Ziel der Richtlinie ist es, Hindernisse für den Binnenmarkt zu beseitigen. Insbesondere sollen die rechtliche Anerkennung elektronischer Signaturen auf Gemeinschaftsebene gewährleistet sowie Beschränkungen des freien Verkehrs von Zertifizierungsdiensten und -produkten zwischen den Mitgliedstaaten vermieden werden. Für die Zertifizierungsdienste gewährleisten Art. 3 und 4 der Richtlinie einen freien Marktzugang in der EG. So dürfen die Mitgliedstaaten die Bereitstellung von Zertifizierungsdiensten nicht von einer vorherigen Genehmigung abhängig machen. Die Elektronische Signatur nach der EU-Richtlinie ist ferner nicht an ein bestimmtes Verschlüsselungssystem gebunden und kann nach Wahl des Zertifizierungsdienstleisters ausgewählt werden. Das zentrale Sanktionsmittel für die Einhaltung der Sicherheitsanforderungen ist eine Haftung der Diensteanbieter nach Art. 6 der Richtlinie. Bei so genannten fortgeschrittenen elektronischen Signaturen, die auf einem qualifizierten Zertifikat beruhen und von einer sicheren Signaturerstellungseinheit erstellt wurden, werden gemäß Art. 5 Abs. 1 der Richtlinie weitere rechtliche Folgen an deren Verwendung geknüpft. So ist z.B. nach Art. 5 Abs. 1 lit. a Sig-Ril die Gleichstellung mit handschriftlichen Unterschriften in Bezug auf Daten, die auf Papier vorliegen, sicherzustellen.

Lange vor der europäischen Richtlinie war bereits das deutsche Signaturgesetz (SigG) als Art. 3 des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) am 1. August 1997 in Kraft getreten[4]. Die digitale Signatur nach dem Signaturgesetz ist grundsätzlich technikoffen, basiert auf einem asymmetrischen Kryptoalgorithmus und muss vor Verwendung durch eine akkreditierte Zertifizierungsstelle geprüft werden. Im Gegensatz zur Richtlinie ist nach § 4 SigG der Betrieb einer Zertifizierungsstelle von einer Genehmigung durch die Regulierungsbehörde abhängig. Regelungen zu Haftung oder Rechtsfolgen sind im Signaturgesetz nicht enthalten. Entsprechend des Beschlusses des Deutschen Bundestages vom 11. Juni 1997[5] hat die Bundesregierung nach zwei Jahren einen Bericht mit Empfehlungen zur Evaluierung des Signaturgesetzes verfasst[6].

---

1 *KOM* (1998) 297 endg. Abl. EG Nr. C 325/5 v. 23.10.1998.

2 *Gemeinsamer Standpunkt (EG)* Nr. 28/1999, Abl. EG Nr. C 243/02 vom 27.08.1999.

3 *Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*, Abl. L 13 vom 19.01.2000; zu den im Wesentlichen inhaltsgleichen früheren Fassungen *Gravesen/Dumortier/van Eecke*, Die europäische Signaturrichtlinie – regulative Funktion und Bedeutung der Rechtswirkung, in: Multimedia und Recht (MMR) 1999, 577 ff.

4 *BGBl.* I, S. 1870.

5 *BT-Drs.* 13/7935.

6 Siehe Bericht der Bundesregierung über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des Informations- und Kommunikationsdienste-Gesetzes – IuKDG – *BT-Drs.* 14/1191.

Sowohl die Signaturrichtlinie als auch der Evaluierungsbericht erfordern nun Anpassungen des Signaturgesetzes. Das Bundeswirtschaftsministerium (BMWi) hat mittlerweile einen Diskussionsentwurf für ein Gesetz zur Änderung des Signaturgesetzes vorgelegt[7]. Die wesentlichen Anpassungsbedarfe und ihre jeweilige Umsetzung nach dem gegenwärtigen Stand sollen hier kurz dargestellt werden[8]:

Erforderlich ist zum einen ein Wegfall der Genehmigungspflicht für Zertifizierungsstellen. Im Diskussionsentwurf wird dies in § 4 festgeschrieben, mit dem Ziel, das Sicherheitsniveau des Signaturgesetzes durch die Einführung einer freiwilligen Akkreditierung für Zertifizierungsstellen weiter zu gewährleisten. Hieran könnten insbesondere öffentlich-rechtliche Formerfordernisse anknüpfen (vgl. auch Art. 3 Abs. 7 Sig-Ril), soweit die spezifische Verwaltungsanwendung dies erfordert.

Die Sig-Ril erfordert weiter die Regelung von Rechtsfolgen für fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und von einer sicheren Signaturerstellungseinheit erstellt wurden (Art. 5 Abs.1 Sig-Ril). In Deutschland ist nur eine Anpassung des Schriftformerfordernisses erforderlich. Die Beweiswirkung ist durch die Möglichkeit des Augenscheinbeweises bereits erfüllt. Jedoch wird das zukünftige Signaturgesetz nicht die Anpassung der Formvorschriften regeln. Während die diesbezüglichen verwaltungsrechtlichen Anpassungsbedarfe erst sehr zögerlich in Angriff genommen werden, existiert hier für das Privatrecht bereits seit längerem ein Entwurf. Nach dem Entwurf zur Anpassung der Formvorschriften des Privatrechts[9] soll mittels Änderung des § 126 Abs. 3 BGB die elektronische Form (Namensunterzeichnung und digitale Signatur, vgl. § 126a Abs. 1 BGB nF) der schriftlichen Form gleichgestellt werden, solange nichts anderes bestimmt ist[10]. Eine absehbare entsprechende Änderung des BGB bliebe jedoch auf die verwaltungsrechtlichen Formvorschriften ohne Wirkung[11].

Außerdem ist eine Haftungsregelung sowie eine Deckungsvorsorge für Zertifizierungsdiensteanbieter in das Signaturgesetz aufzunehmen. Diese sind in den §§ 11 und 12 des Diskussionsentwurfs enthalten.

Des Weiteren bedarf es der Ausweitung der spezifischen Datenschutzregelung auf Zertifizierungsstellen, die keine qualifizierten Zertifikate ausstellen (vgl. §§ 14 und 1 Abs. 3 des Diskussionsentwurfs). Schließlich ist die Beseitigung der Unsicherheit hinsichtlich der Möglichkeit der Errichtung von Registrierungsstellen als Ergebnis der Evaluierung des Signaturgesetzes wünschenswert. Eine solche Klarstellung ist in § 4 Abs. 5 des Diskussionsentwurfs erfolgt.

Die Verabschiedung des 1. SigÄndG ist für Herbst 2000 und das In-Kraft-Treten zum 1. Januar 2001 geplant.

---

7 Abzurufen unter http://www.iid.de/iukdg/gesetz/DEntwurf07_12-04.PDF (Stand: 5.5.2000).

8 Vgl. dazu auch umfassend *Roßnagel*, Europäische Signatur-Richtlinie und Optionen ihrer Umsetzung, MMR 1999, S. 261 ff.

9 Vgl. Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr vom 19.5.1999, abzurufen unter http://www.dud.de/dud/files/bgbe0599.zip (Stand: 5.5.2000). Mittlerweile ist ein weiterer Entwurf vorhanden, der jedoch noch nicht öffentlich gemacht worden ist.

10 Die Sig-Ril verlangt hier nur leichte Modifikationen des Gesetzentwurfs.

11 Siehe *Eifert/Schreiber*, „Elektronische Signatur“ und der Zugang zur Verwaltung, MMR 6/2000 (im Erscheinen). Anders *Deutscher Städtetag*, Digitale Signatur auf der Basis multifunktionaler Chipkarten, 1999, S. 47.

Bei der Realisierung eines geeigneten Key-Managements ergeben sich verschiedene Probleme, die jedoch eher organisatorischer denn juristischer Natur sind. Dennoch müssen eingesetzte Organisationsstrukturen einer rechtlichen Prüfung unterworfen werden, um sicherzustellen, dass die hohen Sicherheitsanforderungen des Signaturgesetzes und der Signaturverordnung weiterhin eingehalten werden.

1.2 Digitale Signatur – technische Voraussetzungen und Probleme [Autor: Hermann Strack (TÜViT)]

Im Folgenden werden einige zentrale technische Voraussetzungen und zugeordnete Probleme reflektiert, soweit sie nach jetzigem Informationsstand für die Entwicklung in den Städten relevant erscheinen. Wir konzentrieren uns zunächst auf den Themenbereich der digitalen Signatur und beziehen dann weitere Sicherheitsthemen ein.

1.2.1 Einführung

Lösungen, wie sie innerhalb des *MEDIA*@Komm-Projekts entstehen sollen, sind aus sicherheitstechnischer Sicht unter verschiedenen Kategorien von Sicherheitszielen bzw. zugehörigen Lösungen zu betrachten. Diese Kategorien sind folgende:

- Vertraulichkeit – Schutz vor unbefugter Preisgabe von Informationen;
- Authentizität und Integrität – Nachweis der Urheberschaft und der Unmanipuliertheit von Informationen (Schutz vor unbemerkter unbefugter Veränderung von Informationen);
- Zugriffschutz/-kontrolle – Schutz vor unbefugten Zugriffen auf gespeicherte Informationen;
- Verfügbarkeit – Schutz vor unbefugter Vorenthaltung von Informationen oder Betriebsmitteln;
- Teilweise: Anonymität/Pseudonymität – Schutz vor Aufdeckung des Urhebers oder Senders einer Information.

Es stehen unterschiedliche sicherheitstechnische Maßnahmen bereit, um den Anforderungen nach Vertraulichkeit, Authentizität, Integrität, Zugriffsschutz und Verfügbarkeit gerecht zu werden. Diese sind in einer Organisation mittels eines Sicherheitskonzepts zu behandeln. Im Folgenden werden einzelne Maßnahmen aufgeführt, die zur Erfüllung der genannten Bewertungsaspekte dienen können:

- Die Vertraulichkeit wird im Allgemeinen durch Verschlüsselungsverfahren erreicht. Hier sind symmetrische und asymmetrische Verschlüsselungsverfahren sowie die zugehörige Infrastruktur (z.B. für Schlüsselmanagement) zu nennen. Bei Verschlüsselungen für gespeicherte Daten insbesondere im nicht-privaten Bereich werden im Allgemeinen abgesicherte Wiederherstellungsverfahren für verschlüsselte Daten erforderlich, um vor Verfügbarkeits- und Totalverlusten zu schützen.
- Hilfsmittel bei der Sicherstellung der Integrität und Authentizität von ausgetauschten Daten sind asymmetrische Verschlüsselungsverfahren und so genannte Public-Key-Verfahren im Umfeld digitaler Signaturen.
- Hilfsmittel des Zugriffsschutzes sind die Benutzerauthentisierung (in Einzelfällen auch die Systemauthentisierung gegenüber dem Benutzer), die Zugriffsrechteadministration und entsprechende Zugriffskontrolle (in Betriebssystemen, aktiven Netzkomponenten wie Firewalls, Datenbanken, Anwendungssystemen), gegebe-

nenfalls kombiniert mit Verschlüsselungsverfahren und zugehöriger Infrastruktur sowie Protokollierungsverfahren.

- Hilfsmittel zur Erreichung von Anonymität und Pseudonymität sind entsprechende vertrauenswürdige Anonymisier- und Pseudonymisier-Einrichtungen (z.B. MIXe, Re-Mailer), die Identitätsinformationen aus eingereichten Nachrichten entfernen bzw. pseudonym ersetzen. In vielen Anwendungsfällen ist der Zugang zu diesen Einrichtungen mit einer Berechtigungsprüfung vor der eigentlichen Anonymisierung/Pseudonymisierung zu versehen (Beispiel: Feststellung der Wahlberechtigung vor der anonymen Stimmabgabe), damit nicht beliebige Personen (auch mehrfach) teilnehmen können.
- Die Verfügbarkeit von Diensten ist nur innerhalb eines umfassenden Sicherheitskonzepts realisierbar, wobei Aspekte wie Firewall-Lösungen zu integrieren sind.
- Generell bedürfen alle vorgenannten Maßnahmen verschiedenster Unterstützungen in ihrer Einsatzumgebung (z.B. baulicher/physischer, personeller, organisatorischer, IT-integrationsbezogener, netzwerkbezogener Art), die aufeinander abgestimmt in einem Sicherheitskonzept oder mindestens in Benutzerrichtlinien bereitgestellt werden.
- Immer dann, wenn es wichtig ist, Dritte von der „Güte“ der geplanten oder bereits eingerichteten Sicherheit zu überzeugen, sei es im Bereich von Komponenten, Einzelmaßnahmen oder gesamtem Sicherheitskonzept, empfiehlt sich die unabhängige Überprüfung durch vertrauenswürdige Stellen mit einem Prüfzeugnis möglichst nach offen gelegten Prüfkriterien. Unter Effektivitätsgesichtspunkten empfiehlt sich dabei eine möglichst frühzeitige Beteiligung dieser externen Stellen im Planungsprozess.

1.2.2 Verschlüsselung

Die Vertraulichkeit wird im Allgemeinen durch symmetrische und asymmetrische Verschlüsselungsverfahren erreicht. Kommt es auf einen hohen Datendurchsatz an oder sind die Operationen zeitkritisch, z.B. bei der Online-Leitungsverschlüsselung, so sind symmetrische Verfahren vorzuziehen. Hierbei ist es allerdings notwendig, dass alle Kommunikationspartner ein gemeinsames Geheimnis verwenden. Dieses Geheimnis ist gesichert zu übertragen und sicher aufzuwahren. Im Allgemeinen werden solche Geheimnisse mittels asymmetrischer Verschlüsselungsverfahren (so genannten Hybridverfahren, oft ohne dass der Benutzer es bemerkt) ausgetauscht und sind nur für einen Verbindungsaufbau gültig (vgl. Session-Key, Replay-Attacke). Asymmetrische Verschlüsselungsverfahren werden in der Regel verwandt, um Offline-Verschlüsselungen durchzuführen. Hier sei als Beispiel die Dokumentenverschlüsselung genannt. Solche asymmetrisch verschlüsselten Dokumente können dann z.B. auf einem Server abgespeichert werden oder per E-Mail versandt werden. Bei allen Verschlüsselungsverfahren ist zu beachten, dass neben der Auswahl eines geeigneten Verfahrens der Parameterwahl (z.B. Schlüsselwahl) eine entscheidende Bedeutung zukommt. Auch das Schlüsselmanagement ist ein nicht zu unterschätzender Aspekt – insbesondere bei den symmetrischen Verschlüsselungsverfahren –, um die Sicherheit des Gesamtverfahrens zu garantieren (vgl. Sicherheitskonzept).

Während Signaturschlüssel personenbezogen gewählt werden, kann es insbesondere im Kontakt von Bürger zu Behörde oder von Kunde zu Firma von Vorteil sein, auf Seiten der Behörde oder Firma nicht personenbezogene, sondern rollen- oder funktionsbezogene Verschlüsselungsschlüssel anzubieten, damit mehrere Mitarbeiter in Arbeitsteilung die eingesandte verschlüsselte Information entschlüsseln können.

Gerade bei Verschlüsselung gespeicherter Objekte ist es, insbesondere im nicht-privaten Bereich (Firmendokumente usw.), im Allgemeinen notwendig, abgesicherte Wiederherstellungsverfahren für verschlüsselte Daten vorzusehen, um vor Verfügbarkeits- und Totalverlusten bei Schlüsselverlust oder Schlüssel-Nichtverfügbarkeit zu schützen.

1.2.3 Digitale Signaturen und Public-Key-Infrastruktur (PKI)

Die Sicherstellung der Authentizität und Integrität über offene Netze ausgetauschter Daten stellt einen entscheidenden Aspekt für die Akzeptanz und Nutzbarkeit von Dienstleistungen in offenen Netzen (z.B. Internet) dar. Nur wenn sichergestellt wird, wer eine Dienstleistung anfordert bzw. bereitstellt, kann Vertrauen in deren Erbringen geschaffen werden. Werden Gebühren für eine Dienstleistung fällig oder gar Waren bestellt, so kann eine Abrechnung nur auf Basis eines authentischen und integren Datenaustauschs erfolgen.

Hilfsmittel bei der Sicherstellung der Authentizität und Integrität ausgetauschter Daten sind asymmetrische Verschlüsselungsverfahren und so genannte Public-Key-Verfahren im Umfeld digitaler Signaturen. Das Verfahren einer digitalen Signatur basiert auf einem asymmetrischen Verschlüsselungsverfahren mit einem privaten (Signatur-) Schlüssel und einem öffentlichen Schlüssel. Dieses Schlüsselpaar ist einander zugeordnet und muss speziellen mathematischen Eigenschaften genügen. Dies wird z.B. durch die Erzeugung dieses Schlüsselpaars in einer Zertifizierungsstelle sichergestellt. Zudem muss der private Signaturschlüssel streng geheim aufbewahrt werden. Dies wird in der Regel durch die vertrauenswürdige Einbringung und zugriffsgeschützte Speicherung in einer geeigneten Prozessorchipkarte sichergestellt. Nur nach erfolgreicher Identifizierung und Authentisierung wird der private Signaturschlüssel intern auf der Chipkarte angewandt. Der private Signaturschlüssel darf dabei nicht aus der Chipkarte ausgelesen werden können. Dies wird durch die Sicherheitstechnik des Prozessors auf der Chipkarte und dem zugehörigen Betriebssystem sowie die vertrauenswürdige Personalisierung der Chipkarte (Einbringen des geheimen Signaturschlüssels) – z.B. in einer Zertifizierungsstelle – garantiert.

An dieser Stelle wird deutlich, dass der Endbenutzer Vertrauen in die Chipkartentechnik und in die geeignete Schlüsselpaarerzeugung sowie Personalisierung haben muss. Daher dürfen nach SigG/SigV nur Chipkartensysteme zum Einsatz kommen, die überprüft und deren Eignung bestätigt wurden. Ebenso ist neben der eigentlichen Chipkarte, d.h. dem Prozessor und Betriebssystem, die Schlüsselerzeugung und Vorpersonalisierung (Einbringen des geheimen Signaturschlüssels in das Filesystem der Chipkarte) einer Eignungsprüfung und Bestätigung zu unterziehen.

Zurzeit werden die Schlüsselpaare im Sicherheitsbereich einer Zertifizierungsstelle erzeugt, auf ihre mathematische Eignung überprüft und vertrauensvoll in das Filesystem

geeigneter Chipkarten eingebracht. Die derzeit bestätigten Verfahren sind solche der Deutschen Telekom AG (TeleSec) und der Deutschen Post AG (PostCom). Die Idee anderer Ansätze ist es – neben der Speicherung und Anwendung des geheimen (privaten) Signaturschlüssels –, auch die Erzeugung und mathematische Eignungsprüfung auf eine Prozessorchipkarte zu integrieren. Solche Ansätze befinden sich zurzeit in sicherheitstechnischer Bewertung. Eine solche Schlüsselerzeugung auf der Chipkarte hat – neben den Schwierigkeiten bei der technischen Realisierung – mehrere Vorteile. Zum einen wird kein spezieller Sicherheitsbereich bei der Erzeugung des Schlüsselpaars benötigt, da der private Signaturschlüssel die Chipkarte nicht verlassen muss. Zum anderen kann die Schlüsselerzeugung dezentral und somit vor Ort bei einer Chipkartenbeantragung erfolgen. Einen wesentlichen Betrachtungsgegenstand innerhalb des Sicherheitskonzepts stellt die Rolle der Zertifizierungs- und Registrierungsstellen dar. Wird auf bestätigte Stellen zurückgegriffen, so können die bei deren Bestätigung vorgelegten Konzepte integriert werden, ansonsten sind eigene Konzeptlösungen zu qualifizieren und zu bestätigen. Die Sicherheit des Gesamtverfahrens muss aufrechterhalten bleiben.

1.2.4 Funktionsweise digitaler Signaturen

Die Grundidee der digitalen Signatur sieht wie folgt aus: Ein Text, der digital signiert werden soll, wird aus Effizienzgründen mittels einer so genannten Hashfunktion kryptographisch komprimiert („Einweg“-Komprimat) – praktisch nicht wiederherstellbar oder bezüglich des Komprimats vorhersagbar. Das eindeutige Ergebnis dieser Komprimierung, der so genannte Hashwert, wird mit dem privaten Signaturschlüssel verschlüsselt. Die Verschlüsselung erfolgt auf der Chipkarte. Das Verschlüsselungsergebnis wird als digitale Signatur dem Ursprungstext zugeordnet. Soll die Integrität eines signierten Textes nachgewiesen werden, so geht man wie folgt vor: Der Text wird wiederum komprimiert, das Ergebnis ist erneut ein eindeutiger Hashwert. Die dem Text zugeordnete Signatur (verschlüsselter Hashwert) wird mittels des öffentlichen Schlüssels entschlüsselt und mit dem zuvor berechneten Hashwert verglichen. Bei einer Übereinstimmung garantieren das mathematische Verfahren und die geeignete Schlüsselauswahl die Authentizität und Integrität des Ursprungstextes.

Um aber den Unterzeichner (Aussteller der digitalen Signatur) identifizieren zu können, bedarf es eines weiteren Hilfsmittels, des so genannten Zertifikats. Ein Zertifikat ist im Wesentlichen eine digitale Bescheinigung über die Zuordnung zwischen einer Person und einem Signaturschlüsselpaar. In einem Zertifikat ist dazu der einer Person zugeordnete öffentliche Schlüssel integriert. Ein Zertifikat wird von einer Zertifizierungsstelle ausgestellt und von dieser digital signiert. Bisher zugelassene Zertifizierungsstellen, d.h. überprüfte und bestätigte Zertifizierungsstellen, sind jene der Deutschen Telekom AG (TeleSec) und der Deutschen Post AG (PostCom). Die Zertifikate dieser Zertifizierungsstellen werden wiederum von der „Wurzelzertifizierungsstelle“ nach deutschem Signaturgesetz, der Regulierungsbehörde für Telekommunikation und Post (RegTP), digital signiert. Damit wird nun die „Zertifikatskette“ nach „oben“ beendet, d.h., die Zertifikate der RegTP werden mit den jeweiligen Signaturschlüsseln der RegTP untereinander signiert und „via Papier“ im Bundesanzeiger vertrauenswürdig veröffentlicht.

Neben der Ausstellung von Signaturkarten und Zertifikaten *verwalten* die Zertifizierungsstellen auch die Zertifikate (z.B. Anbieten eines Sperrdienstes); außerdem informieren sie über die ausgestellten Zertifikate – insbesondere über deren Gültigkeits- und Sperrstatus. Nach dem Signaturgesetz bieten Zertifizierungsstellen auch einen Zeitstempeldienst für vom Benutzer eingesandte Daten an. Die Zertifizierungsstellen offerieren häufig auch Zusatzdienstleistungen wie die Ausstellung weiterer Schlüsselpaare (neben dem gesetzlich geregelten Signaturschlüsselpaar), etwa zur Verschlüsselung oder Zugangsauthentisierung.

1.2.5 Technische Voraussetzungen und Probleme

1.2.5.1 Zertifizierungsstellen nach Deutschem Signaturgesetz

Die Ausgangssituation in Deutschland ist für potenzielle Nutzer der digitalen Signatur nach deutschem Signaturgesetz seit der CeBIT 2000 dadurch gekennzeichnet, dass jetzt zwei verschiedene von der Regulierungsbehörde (RegTP) genehmigte Zertifizierungsstellen als Infrastruktur zur Verfügung stehen:

- die Zertifizierungsstelle der Deutschen Telekom AG (DTAG) (die Betriebsaufnahme nach Genehmigung durch die RegTP erfolgte Anfang 1999);
- die Zertifizierungsstelle der Deutschen Post AG (DPAG) (die Genehmigung der RegTP wurde am 24.2., die Betriebsaufnahme schließt sich an).

Zum jetzigen Zeitpunkt muss (mangels vorliegender Detailinformationen) befürchtet werden, dass Zertifikate und Dienstleistungen der genehmigten Zertifizierungsstellen sowie zugeordnete Benutzerinfrastrukturlösungen anfangs nicht interoperabel sein werden (dies ist nach Signaturgesetz auch nicht obligatorisch). Allerdings gibt es bereits eine Initiative „ISIT“ von interessierten privatwirtschaftlichen Zertifizierungsstellen zu Interoperabilitätsfragen, die Entwürfe zur Zertifikatsstandardisierung vorgelegt hat.

Aus Benutzersicht könnten nun folgende Interoperabilitätsfragen von Interesse sein:

- Sind Zertifikats-, Attributzertifikats- und Zeitstempelformate verschiedener Zertifizierungsstellen einheitlich, sodass sie potenziell mit einem einzigen Tool angezeigt und bezüglich der Signatur geprüft werden können?
- Sind die Verzeichnisdienst- inklusive Sperrdienstschnittstellen für Zertifikatsprüfungen (auch hinsichtlich selbstbeschränkter Zertifikate oder entsprechender Attributszertifikate) bzw. Zeitstempeldienst-Schnittstellen einheitlich, sodass sie potenziell mit einem einzigen Tool bearbeitet werden könnten?
- Wie kann der Benutzer derzeit aus den gesetzlichen Bestätigungsinformationen für Komponenten und Zertifizierungsstellen die für ihn notwendigen Interoperabilitätsinformationen ableiten?

1.2.5.2 Benutzerinfrastruktur nach Deutschem Signaturgesetz

Zu den Möglichkeiten des Benutzers, sich mit nach Signaturgesetz bestätigten Benutzerinfrastrukturlösungen auszustatten, bietet sich ein uneinheitliches Bild. Diese Komponenten (Hard- und Software) umfassen für mit bestätigten Chipkarten ausgestattete Endbenutzer derzeit Komponenten zur Kommunikation zwischen Rechner und Chipkarte, zur Eingabe der PIN für die Chipkarte, zur Verifizierung/Prüfung von Signaturen und der Gültigkeit von Zertifikaten, zur gesicherten Anzeige zu signierender Daten sowie schließlich zur Signaturerstellung selbst.

Zum einen enthält die Liste der bestätigten Komponenten nach Signaturgesetz für Benutzer unter www.regtp.de (Stand 13.3.2000), die jedoch offenbar zeitlich den amtlichen Bundesanzeigerveröffentlichungen nachfolgt, die bei den zuständigen Bestätigungsstellen wie z.B. TÜViT und Debis sowie die bei den Herstellern wie der Utimaco AG selbst bestätigten Komponenten, die jedoch gegebenenfalls hinsichtlich der Verwendbarkeit keinem der oben genannten Zertifizierungsstellen-Anbieter zuzuordnen sind.

Zum anderen erfährt man auf der Verzeichnisdienstseite der DTAG im WWW (Stand 13.3.2000), dass sich die betreffende Benutzerkomponente der DTAG noch in der Bestätigung nach Signaturgesetz befindet. Möglicherweise steht also derzeit (13.3.2000) noch keine bestätigte Endbenutzerkomponente nach Signaturgesetz zur Verfügung, die mit einer in Betrieb befindlichen Zertifizierungsstelle nach Signaturgesetz zusammenarbeitet.

Eine klarere Informationspolitik im Vorfeld von Bestätigungen wäre dringend wünschenswert – und zwar sowohl hinsichtlich der Benutzerinfrastrukturen für den Endbenutzer wie auch im Hinblick auf Interoperabilitätsfragen.

So ist es als problematisch anzusehen, wenn dem Benutzer keine nach Signaturgesetz vorgesehenen bestätigten Komponenten zur Verfügung gestellt werden und er nicht über die Konsequenzen des Fehlens dieser Komponenten unterrichtet wird.

1.2.5.3 EU-Richtlinie zu elektronischen Signaturen

Die EU-Richtlinie für elektronische Signaturen schafft de facto die Möglichkeit mehrerer Stufen von Signaturen – also differierender Sicherheitsstandards für unterschiedliche Anwendungsfelder – mit verschiedenen rechtlichen und auch technischen Implikationen sowie einer Reihe offener Fragen hierzu.

So bestehen in Kurzform nach der EU-Richtlinie folgende Optionen für elektronische Signaturen:

- elektronische Signatur (eSig) – auch nicht-kryptographisch realisierbar;
- fortgeschrittene eSig (FeSig), gegebenenfalls unter Verwendung von Public-Key-Kryptographie;
- FeSig mit qualifiziertem Zertifikat/ZS (FeSigQ) => Haftung der ZS
- FeSigQ mit sicherer Signaturerstellungs-Einheit (FeSigSQ) <=> handschriftlicher Unterschrift (Äquivalent)

- FeSig mit freiwillig akkreditierter ZS (FeSig...A), z.B. nach deutschem Signaturgesetz;
- eSig+ mit zusätzlichen Anforderungen im nationalen öffentlichen Bereich.

Zusammenfassend lässt sich sagen, dass auch nach den höchsten Stufen gemäß der EU-Richtlinie nicht die obligatorisch geregelte technische Sicherheit nach deutschem Signaturgesetz erreicht wird.

Zwar bleibt letztere immerhin als Einbettung möglich, indem die bisherigen Anforderungen nach deutschem Signaturgesetz via freiwilliger Akkreditierung durchgesetzt und den Produkten zugeordnet werden könnten. Es bleiben jedoch einige offene Fragen:

- Einfache (auch nicht-kryptographische) digitale Signaturen dürfen nicht als Beweismittel bei Gericht ausgeschlossen werden, obwohl sie sicherheitstechnisch potenziell sehr leicht fälschbar sind und mangels geregelter Mindestanforderungen an die Infrastruktur und deren Betrieb sicherheitstechnisch kaum klare Ansatzpunkte für eine Beweiserhebung mit verlässlichen Indizien existieren (vgl. nachfolgende Punkte).
- Erst bei fortgeschrittenen Signaturen (FeSig) kann gegebenenfalls von durch Public-Key-Kryptographie fundierten Signaturen ausgegangen werden. Die obligatorischen Vertrauenswürdigkeitskriterien für Komponenten und Zertifizierungsstellen nach EU-Richtlinie sind allerdings – soweit bisher überhaupt veröffentlicht (s. Anhang der EU-Richtlinie: nur einige Sicherheitsanforderungen dort) – wesentlich schwächer ausgebildet als nach deutschem Signaturgesetz:
- Nur die Komponente „Signaturerstellungs-Einheit“ soll sicherheitstechnisch geprüft werden, jedoch bei noch offenen technischen Kriterien.
- Bezüglich anderer Komponenten genügen Herstellererklärungen (inklusive Verweis auf Standards).
- Selbstbeschränkungsmöglichkeiten des Nutzers sind erst bei qualifizierten Zertifikaten vorgeschrieben.
- Die obligatorische Prüfung und Genehmigung der Eignung verwendeter Kryptoalgorithmen und Parameter (wie nach SigG/SigV erforderlich) ist nicht vorgesehen, sondern deren Auswahl bleibt dem Anbieter überlassen.
- Anbieter qualifizierter Zertifikate werden staatlich (oder staatlich beauftragt) hinsichtlich ihrer Zertifizierungsinfrastruktur überwacht, eine vorherige obligatorische Begutachtung vor Betriebsaufnahme im Sinne einer Genehmigung der ZS-Infrastruktur ist jedoch ausdrücklich verboten, die Kriterien der Überwachung bleiben offen.
- Die Zertifikatserteilung an nicht natürliche/juristische Personen erscheint möglich – ohne Klärung sicherheitstechnisch relevanter Infrastrukturfragen.

Aus sicherheitstechnischer Sicht stimmt bedenklich, dass technisch unsichere, einfache Signaturen in ihrer potenziellen Rechtswirkung verstärkt werden (Zulassung als Beweismittel vor Gericht – EU-weit), ohne gleichzeitig klare Fälschungsfolgen mildernde Faktoren im Vorfeld vorzusehen – wie z.B. *nationale* Clearingstellen für Fälschungen; Beschränkbarkeit der Haftung für einfache Signaturen; Aussetzung des Zwanges zum Erscheinen vor Gericht bei offensichtlichen Fälschungen und damit Ersparung von Anwaltskosten und Reisekosten zum Gericht.

Es erscheint stark unverhältnismäßig, dass auch für potenziell unsichere einfachere Signaturen mit möglicherweise EU-weiter (oder gar globaler) Verbreitung in Datennetzen im Streitfalle dem durch eine (einfache) Signaturfälschung Betroffenen die gleichen Belastungen im Rechtsstreit (Reisekosten zum weit entfernten Gericht oder juristische Vertretung/Verteidigung vor einem Gericht im Ausland) auferlegt werden wie heute bei einem Rechtsstreit aufgrund gefälschter handschriftlich unterzeichneter Papiere. Bei einfachen elektronischen Signaturen ist nämlich technisch davon auszugehen, dass sie ohne weiteres mit geringem Aufwand sogar automatisiert gefälscht und Betroffenen untergeschoben werden können. Weiter bleibt zu bedenken, dass bei einfachen Signaturen sogar überhaupt keine Zertifizierungsstelle oder bei geringerwertigen kryptographischen Signaturen nur eine Zertifizierungsstelle mit unbestimmter Mindest-Sicherungsinfrastruktur hinsichtlich Registrierung und Dokumentation einschaltbar ist, sodass in diesen Fällen nicht einmal mit Hilfe einer Zertifizierungsstelle das Unterschieben von Signaturen aufgeklärt werden kann. Das Fehlen klarer Beschränkungsregelungen für einfachere Signaturen birgt für den Benutzer – und unter Umständen auch für den Nicht-Benutzer – ein nicht absehbares oder beherrschbares Risiko.

Was Sicherheitsprüfungen für höherwertige Signaturen anbelangt, ist daran zu erinnern, dass sich im Bereich der IT-Sicherheit allgemein und auch im PKI-Umfeld nachträgliche sicherheitstechnische Prüfungen ebenso wie Hersteller-Selbsterklärungen in der Regel als nicht dem Stand der Technik und Qualitätssicherung sowie des Wissens entsprechend erwiesen haben. Solche Vorgehensweisen verzichten, verfahrenstechnisch gesehen, auf die Vorteile eines geregelten entwicklungsbegleitenden Prüfverfahrens nach definierten Kriterien entsprechend dem Stand der Technik.

1.3 Ökonomische Fragen bei der Verbreitung der digitalen Signatur [Autor: Busso Grabow (Difu)]

Zentraler Bestandteil der meisten *MEDIA*@Komm-Projekte ist der Einsatz der digitalen Signatur. Der Erfolg oder Misserfolg der Projekte hängt damit nicht nur davon ab, wie in den drei Preisträgerträgerstädten die Diffusion und Akzeptanz der digitalen Signatur voranschreiten, sondern auch davon, wie und in welchen „Spielarten" sich die Anwendung der digitalen Signatur generell, also außerhalb der *MEDIA*@Komm-Projekte, durchsetzt. Deswegen werden dazu aus ökonomischer Perspektive einige Annahmen getroffen.

Die Verbreitung der digitalen Signatur, der entsprechenden Hard- und Software sowie Dienstleistungen wird den Marktgesetzen gehorchen – auch wenn die Impulse zu ihrer Einführung aus dem politischen Raum kommen. Dabei gelten weniger die Marktregeln der klassischen Mikro- und Makroökonomie, sondern eher die Gesetze der Internet- oder Netzwerk-Ökonomie (wie auch immer man die Wirtschaft der Informationsgesellschaft bezeichnen will). Die Netzwerk-Ökonomie beschreibt die ökonomischen Funktionsmechanismen auf Märkten, in denen erhebliche Netzeffekte auftreten[12].

Nach den Regeln der klassischen Ökonomie sinkt der Wert von Gütern, je mehr von diesen auf dem Markt sind. In der Netzwerk-Ökonomie steigt dagegen der Wert des Gutes mit der Verbreitung; auch wenn der materielle Wert sinkt, erhöht sich der Nutzwert überproportional. So genannte „positive Feedbacks" führen dazu, dass mit zunehmender Teilnehmerzahl an Netzwerken deren Attraktivität steigt – und dadurch der Wert für neue Nutzer, an diesem Netzwerk teilzunehmen[13]. Dabei wächst der Wert eines Netzwerks mit der Zahl der Nutzer exponentiell[14]. Man unterscheidet zwischen dem direkten Netzwerknutzen (nach dem Metcalf'schen Gesetz erhöht jeder weitere Nutzer den Wert des Netzwerks) und dem indirekten Nutzen (durch das Setzen von Quasi-Standards durch verbreitete Netzwerke produzieren immer mehr Wertschöpfungspartner passende Produkte; typisch dafür war das Netzwerkprodukt MS-DOS bzw. MS-Windows).

Im Zusammenhang mit der digitalen Signatur gelten die direkten Nutzeneffekte für das quantitativ wachsende „virtuelle Netzwerk" der Nutzer und der Anbieter von Leistungen, die mit der digitalen Signatur durchgeführt werden. Die indirekten Effekte treten auf, in dem Anbieter passend zu den sich entwickelnden Standards der digitalen Signatur zusätzliche Produkte und Dienstleistungen anbieten.

Einer der Gründe, warum die Geldkarte bisher als Zahlungsmittel kaum genutzt wird, liegt darin, dass der „Schwellenwert", die kritische Größe des virtuellen Netzwerks (Nutzer und Anbieter der Zahlungsdurchführung mittels Geldkarte) noch lange nicht er-

12 Vgl. *Axel Zerdick u.a.*, Die Internet-Ökonomie. Strategien für die digitale Wirtschaft, Berlin u.a. 1999, S. 155 (European Communication Council Report).

13 Der Ökonom Brian Arthur nennt dies das Gesetz der steigenden Skalenerträge; vgl. z.B. *Kevin Kelly*, NetEconomy, München und Düsseldorf 1998, S. 39 ff.; *Stan Davis und Christopher Meyer*, Das Prinzip Unschärfe. Managen in Echtzeit; *Zerdick u.a.*, S. 155 ff.

14 Nach dem so genannten Metcalf'schen Gesetz steigt nach dem Überschreiten einer „kritischen Masse" die Nützlichkeit eines Netzes im Quadrat der Anzahl der Teilnehmer (vgl. z.B. *CONDRINET-Studie*, Kap. 1, http://www2.echo.lu/condrinet/Data/ge_sum.htm vom 21.10.1998). Allerdings ändert sich dieser Zusammenhang nach einer gewissen Verbreitung im Markt; der Nutzen näher sich dann asymptotisch an einen oberen Grenzwert an.

reicht ist[15]. Wenn eine kritische Schwelle erst einmal überwunden ist, wächst die Verbreitung der Produkte, also das Marktwachstum, genauso exponentiell wie der Wert des Netzwerks. Beispiele für erfolgreiche Netzwerkprodukte sind Faxgeräte oder, wie erwähnt, die Softwareprodukte von Microsoft[16].

Ein derzeitiges Verbreitungsdilemma der digitalen Signatur besteht darin, dass durch die Anlaufkosten und die noch nicht realisierten *economies of scale* für Kartenleser und Chipkarten vergleichsweise hohe Preise erzielt werden müssten – zumindest gilt dies noch für Signaturen nach höchstem Standard[17] – im Folgenden „akkreditierte Signaturen“ genannt. Generell gilt für die allgemeine Einführung der digitalen Signatur in Deutschland: Je schneller auch Massenanwendungen realisiert werden, die die Signatur nach dem hohen oder höchsten SigG-Standard benutzen, desto schneller trägt sich auch die Einführung entsprechender Signaturkarten. Natürlich gilt dies auch für Signaturen einfachen Standards; hier sind die Hemmnisse auf der Kostenseite aber vergleichsweise gering. Setzt man mindestens auf den hohen Standard der qualifizierten Signatur, so sind zusätzliche Anreize zu schaffen (durch die geringe Größe des Nutzer- und Anbieternetzwerks sind der Nutzen aber für den Privat- und Unternehmenskunden und damit die Nachfrage bisher nur gering). Dazu gibt es verschiedene Wege:

- Festlegung der Marktpreise von Hard- und Software sowie Dienstleistungen zur digitalen Signatur zunächst unter den Herstellungskosten/Kostendeckungsbeiträgen. Im Falle von Verwaltungsdienstleistungen hieße dies ebenfalls, dass man zunächst keine kostendeckenden Gebühren erheben würde; Subventionierung der Karten und der Hardware, bis der Preis so gering ist, dass die individuelle Kosten-/Nutzen-Relation positiv bewertet wird (Konzept Bremen).

- Implementierung von Zusatznutzen auf der Signaturkarte, die den Nutzen erheblich steigern (Konzepte Nürnberg und Bremen); Problem auch der Ausweitung der Anbieter; Bonussysteme als weiterer Weg.

- Implementierung der digitalen Signatur auf gängige Karten, wie etwa die EC-Karte der Banken und Sparkassen (ist bei allen drei Preisträgern vorgesehen); ist eventuell schwierig mit der Signatur höchsten Standards, wenn sie nicht marktgängig ist (z.B. durch hohe Anforderungen an Lesegeräte).

- Generierung eigener Anwendungen durch die Trustcenterbetreiber bzw. ihre Konzernmütter und andere Konzerngesellschaften (SignTrust will als Trustcenterbetreiber zusammen mit ihrer "Mutter" Deutsche Post AG alle zwei Monate eine neue Anwendung auf den Markt bringen).

- Die Akquisition von Pilot-/Großanwendern durch Trustcenterbetreiber und Chipkartenanbieter (z.B. der Pilotversuch des Landes Niedersachsen und der Deutschen Telekom bzw. ihrer Tochter als Trustcenterbetreiber mit 12 000 Karten).

---

15 Nach Angaben des Geschäftsführers der Unternehmensberatung PaySys wurden mit Geldkarten im ersten Halbjahr 1999 weniger als 0,1 Prozent des Gesamtumsatzes im deutschen Einzelhandel getätigt. Nach seinen Einschätzungen müsste mindestens die 30-fache Summe an Zahlungsvorgängen erzielt werden, um die Wirtschaftlichkeitsschwelle zu erreichen.

16 Vgl. z.B. *Kelly*, S. 49.

17 Fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit erstellt wurde.

- Generierung eigener Anwendungen durch die öffentliche Hand als Protagonist der qualifizierten oder akkreditierten digitalen Signatur.
- Das Setzen von gesetzlichen Grundlagen und Umsetzungszwängen von staatlicher Seite aus (das finnische Beispiel der Umstellung der bisherigen Personalausweise auf Chipkarten mit der elektronischen Signatur ist das weitestgehende Beispiel einer Einführungsstrategie).

Auch für die Durchsetzung der digitalen Signatur und entsprechender Chipkarten gilt die große Bedeutung von Standards. Diese „Kriege der Standards" „können in einen Waffenstillstand (wie bei Modems), ein ‚Unentschieden' (wie bei den heutigen Videospielen) oder in einen Kampf auf Leben und Tod (bei den Videorekordern) münden."[18] Durchaus gute Lösungen können, wenn sie nicht die kritische Marktgröße erreichen, als „Verlierer" vom Markt verdrängt werden, bzw. nie eine wirklich rentable Größenordnung erreichen, wenn sich andere, manchmal sogar schlechtere Standards, am Markt durchsetzen (zu beobachten z.B. bei dem Siegeszug von MS-Windows). Die Standards der Netzwerkgesellschaft werden immer seltener von Standardisierungs- oder Normungsinstitutionen gesetzt, sondern durch Marktentwicklungen oder Verbreitung in Netzwerken erzeugt (z.B. MS-Windows, Acrobat, Real-Audio, Linux usw.).

So kann derzeit noch nicht beurteilt werden, welche Signaturen nach welchen Standards sich in Deutschland, der EU und weltweit durchsetzen werden. Man sollte aber davon ausgehen, dass

- Kompatibilitäten und Interoperabilitäten notwendig sein werden (wie man sie zur Zeit zumindest in Deutschland mit ISIS anstrebt),
- sich nicht unbedingt der „beste" Standard durchsetzt,
- die Nutzung der akkreditierten Signatur von der öffentlichen Hand nicht als Regelfall, sondern nur in einzeln zu begründenden Fällen vorgeschrieben werden kann und
- es vermutlich keinen deutschen Sonderweg auf Dauer geben wird. „Proprietäre Systeme" sind in der offenen Netzwerkgesellschaft zum Scheitern verurteilt[19].

Es zeigt sich aber auch, dass im Falle einer Vielzahl von Handlungsoptionen im Hinblick auf elektronische Identifikation und Authentitätsprüfung frühe und erste Steuerungsimpulse, wie sie mit dem deutschen Signaturgesetz und der EU-Richtlinie gegeben wurden, die Richtung der Entwicklungen beeinflussen können[20]. Andererseits gilt in der Netzwerkwirtschaft das Prinzip einer gewissen Zufälligkeit von Erfolgen; Markterfolge lassen sich nicht programmieren, es gibt keine eindeutig guten Geschäftsstrategien in schnell wachsenden Märkten.

Grundsätzlich sollte man davon ausgehen, dass in der Langfristperspektive Hard- und Software zur Unterstützung der digitalen Signatur wie nahezu alle Produkte der IuK-Wirtschaft immer leistungsfähiger und gleichzeitig immer billiger werden. Natürlich gilt

18 *Carl Shapiro und Hal R. Varian*, Online zum Erfolg, München 1999, S. 341.
19 Vgl. z.B. *Kelly*, S. 73.
20 Vgl. ebenda, S. 33.

dies in erster Linie für den Standard (bzw. die Plattform), der (die) sich bis dahin durchgesetzt haben wird.

Es ist zu vermuten, dass die Kosten für Karten und Hard- sowie Software für die akkreditierte Signatur zunächst höher sein werden als die Kosten für andere Zertifikate/elektronische Signaturen nach niedrigeren Standards, sofern sie nicht massiv zu Einstiegspreisen abgegeben werden (zu Beginn also nicht kostendeckend sind).

Gleichzeitig ist anzunehmen, dass gleichzeitig große Anbieter mit hohen Stückzahlen von Signaturkarten mit qualifizierter, vor allem aber einfacher Signatur (z.B. als Zusatzapplikation zu Mobilfunkkarten) auf den Markt kommen. Daraus wird sich ein Wettbewerb entwickeln, der auf verschiedenen Ebenen ausgetragen wird (über die Preise, über mögliche Anwendungen und damit über Zusatznutzen, über „Zwangsnutzungen“ usw.), dessen Ergebnis zunächst noch nicht absehbar ist.

2. Online-Dienstleistungen der Verwaltung unter Nutzung der digitalen Signatur

2.1 Verwaltungsmodernisierung [Autorin: Christine Siegfried (difu)]

Ausmaß und Inhalte kommunaler Aufgaben verändern und erweitern sich im Laufe der Zeit kontinuierlich. Bestehende Aufgaben wandeln sich, neue Aufgaben kommen hinzu, alte werden entbehrlich. Gleichzeitig modifiziert sich auch das Leitbild der Kommunalverwaltung; die Ziele einer den heutigen Anforderungen gewachsenen Kommunalverwaltung werden neu definiert[21]. Dies resultiert in erster Linie aus dem Wandel der gesellschaftlichen und wirtschaftlichen Rahmenbedingungen und ist eine Reaktion auf veränderte Problemstellungen und größeren Handlungsdruck wie z.B. durch Globalisierung, Auflösung von Grenzen zwischen öffentlichen und privaten Bereichen und durch immer schnellere technologische Entwicklungen, vor allem im Bereich der Informations- und Kommunikationstechnologie (IuK).

Als Gründe für die vielfältigen Maßnahmen der Verwaltungsmodernisierung[22] auf kommunaler Ebene sind zu nennen der Sparzwang der Kommunen, fehlende Transparenz des Verwaltungshandelns, mangelnde Bürgerfreundlichkeit sowie auch fehlende Motivation bei der Mitarbeiterschaft. Grundsätzliche Ziele der Bemühungen um Modernisierung von Verwaltungsstrukturen sind eine Erhöhung von Effizienz und Effektivität sowie eine verstärkte Orientierung auf den Bürger als Kunden der Verwaltung. Auf eine umfassende Beschreibung von Gründen, Zielen und Maßnahmen der Verwaltungsmodernisierung in Deutschland soll an dieser Stelle allerdings verzichtet werden. Die Definition von Produkten, die Einführung von Kosten- und Leistungsrechnung, Budgetierung, Controlling und weitere zentrale Ansatzpunkte sind bereits vielfältig und umfassend beschrieben worden[23].

Vielmehr sollen hier die Ziele des Einsatzes von IuK innerhalb von Kommunalverwaltungen sowie erkennbare Restriktionen auf zwei verschiedenen Ebenen betrachtet werden. Die Nutzung von Informations- und Kommunikationstechnologie auf kommunaler Ebene soll zum einen dazu beitragen, Maßnahmen im Zusammenhang mit der Umsetzung von Modernisierungskonzepten zu unterstützen und Organisationsstrukturen und -verfahren zu verändern. In diesem Fall ist der IuK-Einsatz als Instrument zur Unterstützung solcher Ziele wie Effizienzsteigerung und Kostenersparnis unter dem Blickwinkel der *Binnenwirkung* zu betrachten.

Um dem Anspruch an eine bürgerfreundliche Verwaltung näher zu kommen und den Servicegedanken in den Vordergrund zu stellen, eignet sich der Einsatz von IuK besonders, weil durch die Einrichtung so genannter One-Stop-Government-Punkte und die Trennung von Front- und Back-Offices dem Wunsch des Bürgers nach schneller und unbürokratischer Erledigung von Vorgängen schnell entsprochen werden kann. Schließ-

21 Vgl. z.B. *Kommunale Gemeinschaftsstelle (KGSt),* Das Neue Steuerungsmodell, KGSt-Bericht 5/1993.

22 Der Begriff Verwaltungsmodernisierung ist eher ein Sammelbegriff für unterschiedliche Aktivitäten in mehreren Bereichen, wie z.B. im Haushalts- und Rechnungswesen, in der Organisations- oder auch Personalentwicklung.

23 Vgl. dazu Grabow, B., Information, Kommunikation und Multimedia in den Städten, Band II, Handlungsfelder Wirtschaft und Arbeit, Difu-Materialien, Berlin, in Vorbereitung.

lich ergeben sich durch die neuen technischen Möglichkeiten auch neue Ansätze für Bürgerbeteiligung und Partizipation. Und im Wettbewerb der Kommunen untereinander gelten Internet und Multimedia, technische Infrastruktur und Struktur der lokalen Unternehmen inzwischen als wichtiger Standortfaktor. Insofern hat der Einsatz von IuK auch Auswirkungen auf Standortsicherung und Wirtschaftsförderung in Kommunen. Diese Aspekte beleuchten also eher die *Außenwirkung* des kommunalen IuK-Einsatzes.

Im Folgenden sollen diese beiden Aspekte näher beschrieben, soll auf bereits definierte Ziele, umgesetzte Maßnahmen und beobachtete Restriktionen der Verwaltungsmodernisierung hingewiesen werden. Dargestellt werden zunächst die „Trends", die als Folge des IuK-Einsatzes in der öffentlichen Verwaltung zum heutigen Zeitpunkt erkennbar sind. Im letzten Teil wird auf die Probleme, die mit dem IuK-Einsatz verbunden sind, sowie mögliche Lösungsansätze zu deren Überwindung eingegangen.

2.1.1 Binnenperspektive: Effizienzsteigerung des Verwaltungshandelns

Grundsätzlich wird davon ausgegangen, dass der Einsatz von IuK die Effizienz des Verwaltungshandelns erhöhen und zu Kosteneinsparungen führen kann. Information und Kommunikation, Automatisierung und Einführung von Workflowsystemen sowie Re-Engineering von Verwaltungsprozessen und Veränderungen der Ablauforganisation sind dabei zentrale Schlagworte.

Unter Kostengesichtspunkten ist wohl bisher bei den in den Verwaltungen erprobten Projekten noch keine positive Bilanz zu ziehen. Die Einführung neuer Systeme ist zunächst mit zusätzlichen Kosten und Aufwand verbunden, ohne dass unmittelbar Einsparungen an anderer Stelle erkennbar werden. Allerdings werden an einzelnen Stellen, vor allem bei den so genannten Massenanwendungen wie Auskunft aus dem Einwohnermelderegister, schnelle Einnahmen möglich, die diese Aussage wieder relativieren können. Dann hängt es von der Zahl der Nutzer ab, die solche Dienste nachfragen, und von der Frage, inwieweit solche technisch relativ schnell umzusetzenden Verfahren in umfassendere Pläne von IuK-Einsatz (z.B. Einbindung von Intranet und Internet) eingebettet werden.

2.1.1.1 Kommunikation, Information und Wissensmanagement

In einer Zeit, in der die Ressource „Information und Wissen" für die Stadt- und Wirtschaftsentwicklung immer größere Bedeutung erlangt, ist nur die Ausschöpfung der gesamten lokalen und regionalen Wissensbasis Garant für eine positive Entwicklung[24]. Diese Wissensbasis wird aber erst erschlossen, wenn das jeweils spezifische Know-how einzelner Gruppen – innerhalb der Verwaltung, von Unternehmern, Wissenschaftlern, engagierten Bürgern usw. – zusammengeführt und für die Lösung der komplexen Entwicklungsprobleme von Kommunen mobilisiert werden kann. Voraussetzung

24 Vgl. z.B. *Busso Grabow und Holger Floeting,* Städte in der Dienstleistungs- und Informationsgesellschaft, in: Jürgen Egeln und Helmut Seitz (Hrsg.), Städte vor neuen Herausforderungen, Baden-Baden 1998 (Reihe Wirtschaftsanalysen – Schriftenreihe des Zentrum für Europäische Wirtschaftsforschung/ZEW, Bd. 28).

dafür ist funktionierende Kommunikation. Der Einsatz von IuK kann Kommunikation fördern. Zum einen können bisherige Kommunikationsstränge intensiviert werden, zum anderen ermöglicht das Netz auch, dass neue Gruppen durch das Internet miteinander ins Gespräch kommen.

2.1.1.2 Automatisierung/Workflow

Unter dem Zwang, die Verwaltungsvorgänge mit immer weniger Mitteln und Personal in immer kürzerer Zeit durchzuführen, versprechen automatisierte Prozesse Abhilfe. Automatisierungseffekte spielen beim Einsatz von Informationstechnik eine wichtige Rolle. Die *quantitativen* Aspekte treten heute gegenüber den qualitativen Effekten mehr in den Hintergrund. Komplexe IuK-Anwendungen können zur *qualitativen* Verbesserung der Leistungserstellung der Kommunalverwaltung eingesetzt werden. Dies würde aber angesichts der Investitions- und Unterhaltungskosten zu einem echten Finanzierungsproblem führen. Mit der Einführung von Workflowsystemen, durch Systematisierung und Integration von Datenbeständen lassen sich erhebliche Produktivitätssteigerungen und Qualitätsverbesserungen erreichen, können Rationalisierungspotenziale besser ausgeschöpft werden.

2.1.1.3 Veränderung der Ablauforganisation/Re-Engineering

Im Sinne einer Outputorientierung der Verwaltung wird ein „zeitnahes“ Verwaltungshandeln angestrebt, also eine Beschleunigung der Bearbeitungszeit, die durch Vernetzung und den Einsatz von geeigneter Software erreicht werden kann. Anstelle des Prinzips der Vorgangsbearbeitung nacheinander werden durch eine parallele Vorgangsbearbeitung erhebliche Zeiteinsparungen möglich. Häufig ist aus dem gemeinsamen Zugriff verschiedener Sachbearbeiter in unterschiedlichen Stadien einer Vorgangsbearbeitung allerdings die Erkenntnis entstanden, dass bei einer grundsätzlich parallelen Bearbeitung von Vorgängen eine Neuorganisation (Re-Engineering) von Prozessabläufen sinnvoll und notwendig ist. Eine wesentliche Erkenntnis aus den Erfahrungen mit der „Ubiquität der Aufgabenwahrnehmung“[25] besteht in der Einsicht, dass durch technischen Möglichkeiten die bestehenden Produktionsabläufe und organisatorischen Strukturen geändert werden und nicht isoliert bestehen bleiben können. Dies gilt übrigens nicht nur für den Einsatz von IuK; unabhängig vom Technikeinsatz ist ein Re-Engeneering von Verfahren schon bei der Koppelung von Aufgaben verschiedener Dienststellen im Rahmen der allgemeinen Verwaltungsorganisation notwendig.

2.1.1.4 Veränderung der Aufbauorganisation

Durch Vernetzung der Abläufe und Bearbeiter entstehen neue Strukturen. Die Einführung von IuK ist dementsprechend kein Selbstzweck, sie verfehlt ihr Ziel, wenn nicht eine grundlegende Neustrukturierung und Verkürzung der Geschäftsprozesse, der Ar-

25 *Heinrich Reinermann*, Wirkungen von Electronic Government, in: Behördenspiegel, Beilage „Effizienter Staat“, Juli 1999, S. B XVI.

beitsorganisation und der Arbeitsteilung erfolgen[26]. Die in der Verwaltung bisher vorherrschende Betonung der Ablauforganisation verliert unter diesem Aspekt an Bedeutung. Die durch IuK-Einsatz mögliche schnelle Erreichbarkeit von Personen, Daten, Verfahren und Objekten macht eine wirksame Organisation nötig, die sich an modernen Formen des Arbeitsprozesses orientiert und Selbstorganisation, Teamarbeit und Selbstverantwortung stärker in den Vordergrund rückt. Dies bedeutet gleichzeitig eine Reduzierung von Hierarchiestufen und verdeutlicht die Notwendigkeit eines kooperativen Führungsstils. Angst vor Autoritäts- und Machtverlust auf der Leitungsebene bzw. beim Führungspersonal ist ein bekanntes und nicht zu unterschätzendes Hemmnis bei der Einführung neuer Arbeits- und Organisationsstrukturen. Dennoch ist wohl langfristig eine Aufhebung der traditionell vertikal-hierarchischen Strukturen zugunsten horizontal vernetzter Organisationsformen zu erwarten[27]. Dazu ist eine Zusammenführung von Datenbeständen und Informationen ebenso notwendig wie eine Analyse der Geschäftsprozesse, aus der sich die Notwendigkeit von Re-Engineering ergibt. Möglicherweise werden durch den Einsatz von IuK auch Rechtsänderungen notwendig; dies muss bei der Konzeption frühzeitig bedacht werden. Alle hier erwähnten Punkte bedürfen einer frühzeitigen Legitimierung durch den Rat und einer Unterstützung seitens der Verwaltungsspitze. Zu bedenken ist, dass auf Führungsebene und im Rat noch immer Vorbehalte gegen einen „übermäßigen“ Technikeinsatz zu verzeichnen sein können. Bei solchen technikfeindlichen Einstellungen können die besten Konzepte für die Nutzung von IuK nutzlos verpuffen.

Derzeit lässt sich in vielen Kommunen eine Institutionalisierung im Zusammenhang mit dem verwaltungsinternen IuK-Einsatz beobachten. Die ursprünglich wohl auf die Initiative einzelner Personen zurückgehenden Aktivitäten werden in Stabsstellen oder Medienbüros zusammengeführt. Kubicek schließt daraus eine höhere Akzeptanz für Medienprojekte innerhalb der Verwaltung. „Aber, und das ist die wesentliche Erkenntnis, eine planvolle, integrierte Zusammenführung des (nach außen gerichteten) Einsatzes von Internet und Multimedia mit (internen) Verwaltungsreformen ist in Deutschland noch nicht üblich.“[28] Zu vermuten ist ein gestiegenes Problembewusstsein bei Führungskräften, das auch und gerade auf den Wettbewerb der Gemeinden untereinander zurückgeführt werden kann. Ein technikfreundliches und aufgeschlossenes Verhalten gegenüber IuK-Einsatz und -Anwendungen führt schnell zu einem positiven Image.

2.1.1.5 Kompetenzbildung in Rat und Verwaltung

Mit der zunehmenden Vernetzung der Verwaltung, dem schrittweisen Zugang zum Internet an den Arbeitsplätzen und der Koppelung von Intranet und Extranet ist es schließlich notwendig, den Mitarbeitern Kompetenz im Umgang mit dem Internet zu vermitteln. Dies bedeutet über Anleitungen zur Bedienung der Hard- und Software hinaus auch Know-how zur Gewinnung von Informationen aus dem Intranet, Internet,

---

26 *Frieder Naschold, M. Oppen und A. Wegener*, Kommunale Spitzeninnovationen. Konzepte, Umsetzung, Wirkungen in internationaler Perspektive, Berlin 1998, S. 79.

27 Vgl. hierzu *Heinrich Reinermann*, Verwaltungsreform und technische Innovationen – ein schwieriges Dauerverhältnis, in: Herbert Kubicek u.a., Multimedia@Verwaltung, Jahrbuch Telekommunikation und Gesellschaft 1999, S. 11-25.

28 Kubicek, ebenda, S. 63.

Datenbanken usw. zu vermitteln und Schulungen zum Thema Umgang mit Informationen durchzuführen. Häufig fehlt aber auch den kommunalen Entscheidungsträgern das Wissen über Bedeutung und Brisanz des Themenfeldes. Bei den Räten, die die erforderlichen strategischen Entscheidungen treffen sollten, gibt es häufig gravierende Informations- und Wissensdefizite. Dies gilt besonders für den schnelllebigen Bereich IuK und Internet. Regelmäßige Weiterbildung von Rat und Verwaltungsspitze sowie die Einführung so genannter Ratsinformationssysteme sind geeignete Ansätze, um diese Defizite zu beheben.

2.1.2 Außenperspektive des IuK-Einsatzes in Verwaltungen

2.1.2.1 Kunden- und Serviceorientierung

Der Einsatz von elektronischen Signaturen und Chipkarten sowie die Möglichkeit des elektronischen Bezahlens können hier zu einer Weiterentwicklung und zu einer größeren Verbreitung solcher Dienstleistungen führen[29]. In welcher Form sich kommunale Online-Dienstleistungen weiter entwickeln und ob sie auf die Akzeptanz der Bürger stoßen, wird sich erst dann herausstellen, wenn die Auswertung konkreter Erfahrungen in den *MEDIA*@Komm-Städten und anderen Kommunen, die auf diesem Gebiet aktiv sind, vorliegt. In allen Fällen ist Aufklärung bei Bürgern und auch innerhalb der Verwaltung notwendig. Zunächst muss das Bewusstsein für die Möglichkeiten und den Nutzen elektronischer Dienstleistungen der Verwaltung geschaffen werden. Darüber hinaus stellt die notwendige technische Ausstattung ein Hemmnis für die Akzeptanz und schnelle Verbreitung von Signaturen dar, denn Chipkarte und Kartenleser müssen auf beiden Seiten (Bürger und Verwaltung) vorhanden sein. Innerhalb der Kommunen muss auch das Schlüsselmanagement geklärt sein, und das Re-Engineering von Verfahren wird notwendig, wenn Dienstleistungen aus einer Hand angeboten werden sollen. Darüber hinaus sind Rechtsfragen zu beachten und zu klären (z.B. die Frage von Schriftformerfordernissen). Schließlich stellt sich die Frage, ob Aufwand und Nutzen in einem angemessenen Verhältnis stehen, d.h., ob der Bürger das teure Angebot auch wirklich nutzt, denn letztlich reduzieren sich die Kontakte eines Bürgers zur Verwaltung auf einige wenige im Jahr.

2.1.2.2 Verstärkte Partizipation

Ein erklärtes Ziel des Einsatzes von IuK in der Verwaltung -- Förderung von Demokratie und Partizipation – entsteht aus dem Anspruch, die Bürger in das lokale Geschehen mit einzubeziehen[30]. Die Transparenz des Verwaltungshandelns soll nicht nur nach innen, sondern auch nach außen wirken. Bürger sollen befähigt werden, sich über das aktuelle Geschehen zu informieren und aktiv am Willensbildungsprozess teilzunehmen – sich in die Politik vor Ort einzumischen. Das Schlagwort Kommunitarismus wird in diesem Zusammenhang oft genannt. Es bezeichnet den Versuch, die Bürger am Ge-

29 vgl. *Herbert Kubicek und M. Hagen*, Internet und Multimedia in der öffentlichen Verwaltung. Gutachten für die Friedrich-Ebert-Stiftung, Bonn 1999.

30 Ebenda, S. 17.

meinwesen aktiv teilnehmen zu lassen und sie zur Mitwirkung am kommunalen Geschehen zu bewegen. Dies kann auf mehrfache Weise geschehen, so z.B. durch ein angemessenes Informationsangebot, durch eine Verwaltung, die aus der Sicht des Bürgers denkt, durch eine stetig zu verbessernde Angebots- und Servicestruktur der Verwaltung, durch Einbeziehen des in der Bürgerschaft vorhandenen Detailwissens sowie durch konkrete Unterstützung von Projekten[31]. Im Gegensatz zu den Beteiligungsdiskussionen der 70er- und 80er-Jahre liegt der Schwerpunkt heutiger Ansätze zur verstärkten Einbeziehung bürgerschaftlichen Engagements nicht auf der Frage, welche Beteiligungsmöglichkeiten (z.B. in der Bauleitplanung) geschaffen werden können, sondern auf dem Konzept, die Bürger aktiv zur Teilnahme zu bewegen.

Die Möglichkeit, sich als Bürger über das Internet zu informieren und z.B. an lokalen Diskussionsforen teilzunehmen, oder auch elektronische Bürgerbefragungen sollen nicht zuletzt einen Beitrag zum Abbau der Politikverdrossenheit leisten. Ob und inwieweit dieser Anspruch erfüllt werden kann, ist derzeit in der Diskussion, ohne dass bereits gesicherte Erkenntnisse – vor allem über die Wirkungen auf lokaler Ebene – darüber vorlägen. Zur Zeit scheint die erste Euphorie wieder gedämpft, zumal die Resonanz bei den Bürgern geringer als erwartet ausgefallen ist. Ob die Beteiligungsmöglichkeiten, die sich theoretisch durch die weitere Verbreitung von PCs und Internetanschlüssen in der Bevölkerung ergeben, ausgeschöpft werden und inwieweit daraus tatsächlich eine aktive Teilnahme am politischen Leben in der Kommune erfolgt, muss noch weiter untersucht werden[32].

Ob durch den Einsatz von IuK ein Mehr an Demokratie möglich wird, ist auch eine Frage des Zugangs zu den neuen Techniken. Die Ausstattung der Bevölkerung mit PC plus Internetanschluss, mit Chipkarten und dem Wissen darüber, was man mit der Technik alles anfangen kann, ist eher gering einzuschätzen. Zum Informationsabruf ist das Internet sicherlich gut geeignet, aber nur für diejenigen, die sich damit schon auskennen. Wer nicht der klassischen Nutzergruppe (männlich, Hochschulabschluss, zwischen 30 und 40 Jahre bzw. zunehmend auch Jugendliche unter 20) angehört, muss im Umgang mit den neuen Medien geschult werden. Der Vermittlung bzw. Erringung von Medienkompetenz muss daher ein gleicher Stellenwert beigemessen werden wie der Technikausstattung und der Frage des öffentlichen Zugangs. Ob sich durch das Internet Politikverdrossenheit abbauen und Wahlbeteiligungen erhöhen lassen, erscheint dennoch fraglich. Kommunen können aber z.B. durch Bereitstellung öffentlich zugänglicher Info-Terminals ihren Beitrag dazu leisten, dass die neuen Medien für jeden zugänglich sind. Durch Aufklärung und gut gestaltete Informations- und Dienstleistungsangebote können die Kommunen schließlich dazu beitragen, dass die Bürger praktische Erfahrungen sammeln können. Ob sie diese Angebote nutzen und sich tatsächlich befähigt und aufgefordert fühlen, am politischen Prozess teilzunehmen, hängt dann vom Bedarf und von Zielen jedes Einzelnen ab. Die Einschätzung der Kommunen, dass ihre Bürger derzeit eher an Informationen als an Online-Dienstleistungen interessiert sind[33], hängt sicher auch damit zusammen, dass erst wenige Anwendungen angeboten werden und daher kaum praktische Erfahrungen gesammelt werden konnten.

---

31 *Hermann Hill*, Das nächste Jahrhundert – Ein Jahrhundert der Kommunen, http://www.dhv-speyer.de/lst/hill/adenaue.htm.

32 Vgl. hierzu auch Kubicek/Hagen, S. 63.

33 Vgl. ebenda.

2.1.2.3 IuK-Einsatz als Standortfaktor

Aus der praktischen Sicht von Entscheidungsträgern in den Kommunen wird im umfassenden kommunalen Handlungsfeld IuK und neue Medien das Ziel „Stärkung des Wirtschaftsstandortes“ meist an vorderster Stelle genannt[34]. Dabei bezieht sich der Einsatz und die Nutzung neuer IuK-Technologien auf verschiedene Ebenen kommunalen Handelns und reicht über den Ausbau kommunaler Netzinfrastrukturen (einschließlich des Angebots von Diensten) über Informations- und Kommunikationsangebote (z.B. Informationen über Gewerbeflächen) bis in den Bereich der Kompetenzvermittlung, z.B. durch Aus- und Weiterbildung sowohl von Entscheidungsträgern in Rat und Verwaltung als auch von IuK-Anwendern in Betrieben. Auch die Förderung von Produkten und Dienstleistungen im IuK- und Medienbereich, von Anwendungen in kleinen und mittleren Unternehmen sowie von Telearbeit und Telekooperationen fällt als Instrument der Standortsicherung und Wirtschaftsförderung unter den Aspekt des Einsatzes von IuK-Technologien auf kommunaler Ebene[35]. Deutlich wird an diesen Beispielen, dass es sich hierbei weniger um die konkrete Nutzung bestimmter Technologien als vielmehr um eine politisch-strategische Nutzung des Potenzials von IuK und Multimedia handelt, die erheblich zur Wirtschaftskraft der Kommune beitragen kann.

Im Bemühen um die Sicherung und Schaffung von Arbeitsplätzen sowie bei der Ansiedlung von Betrieben gilt das gesamte Themenfeld IuK zugleich als harter wie auch als weicher Standortfaktor. Die Bereitstellung hochleistungsfähiger Telekommunikationsverbindungen gehört ebenso dazu wie Informationssysteme, die Auskunft geben über den Standort, abrufbare Informationen über Fördermittel oder andere relevante Informationen auf übergeordneten Ebenen – oder auch die gezielte Fortbildungsmaßnahme im IuK-Bereich und die Vermittlung von Medienkompetenz für kleine und mittlere Betriebe. Die Beteiligung an der Entwicklung neuer Geschäftsfelder wie E-Commerce im Rahmen öffentlich-privat betriebener Shopping-Malls, die in lokale oder regionale Plattformen integriert sind, ist ein relativ neues Handlungsfeld für Kommunen. Inwieweit die Nutzung der neuen Medien durch die Kommunen tatsächlich in Geld messbare Ergebnisse im Sinne z.B. von Ansiedlungserfolgen erbringt, ist kaum nachweisbar. Das Image als anwender- und nutzerfreundliche, den neuen Techniken und Medien gegenüber aufgeschlossene Kommune dürfte aber diverse Standortentscheidungen beeinflusst haben. Im Prinzip gilt für Unternehmen wie für Bürger: einfache, schnelle Behördengänge, rasche und transparente Bearbeitungsvorgänge genießen einen hohen Stellenwert. Online-Dienstleistungen der Verwaltung machen genau dies möglich und erhöhen damit die *Standortqualität* durch Verbesserung der Dienstleistungen der Verwaltung. Der monetäre Nutzen beispielsweise von elektronisch beschleunigten Baugenehmigungsverfahren kann erheblich sein. Und für Unternehmen spielen Schnelligkeit und Verfahrensverkürzung im Nutzenkalkül eine besonders große Rolle.

---

34 So das Ergebnis einer qualitativen Untersuchung 1995; vgl. *Busso Grabow und Werner B. Korte,* Telematik, Teledienstleistungen und Kommunalpolitik, Berlin 1996, S. 9 (Deutsches Institut für Urbanistik, „Aktuelle Information“).

35 Vgl. dazu ausführlich *Busso Grabow*, Information, Kommunikation und Multimedia in den Städten, Band II, Handlungsfelder Wirtschaft und Arbeit, Berlin 2000 (Deutsches Institut für Urbanistik, Materialien, in Vorbereitung).

2.2 Restriktionen bei der Gestaltung der interaktiven Verwaltung [Autorin: Christine Siegfried (Difu)]

Die Handlungspotenziale, Risiken und Hemmnisse einer „interaktiven“ Verwaltung sind vielfältig. Die folgende Übersicht verdeutlicht die bereits beschriebenen Aspekte.

Das wohl schwierigste Kapitel beim Einsatz von IuK in der Verwaltung sind die häufig zu beobachtenden Insellösungen, die nur für Teilbereiche der Verwaltung gültig sind. Diese beziehen nur einzelne Fachbereiche oder -verfahren ein, die Frage nach der Übertragbarkeit auf andere Bereiche unterbleibt. So bleiben Inkompatibilitäten und Medienbrüche bestehen, eine „Gesamtarchitektur“ kann auf diese Weise kaum entstehen. Auch eine Integration des IuK-Einsatzes in das gesamte Verwaltungshandeln, die die „übergeordneten“ Aspekte der Verwaltungsmodernisierung wie Controlling, Auslagerung von Aufgaben oder Kontraktmanagement mit einbezieht, unterbleibt in der Regel. Diese nicht-integrierte Sichtweise verhindert ein umfangreiches strategisches Management, das außer der Hard- und Softwareausstattung auch das Werben für Konzepte, Vermittlung von Medienkompetenz und Mitarbeiterschulungen sowie ein Vorgehen nach dem Baukastenprinzip umfassen sollte.

Von besonderem Interesse sind ohne Zweifel Fragen der Finanzierung, die sich bei der Planung eines IuK-Einsatzes für die Gesamtverwaltung ergeben. Der Investitionsbedarf der Kommunen in diesem Bereich dürfte in den nächsten Jahren deutlich wachsen. Erste Schätzungen gehen davon aus, dass der Finanzierungsbedarf für den Bereich IuK erstmals jenen aus dem Bausektor übertreffen wird

Werden zunächst in Teilbereichen Lösungen modellhaft entwickelt und erprobt, werden entsprechende Mittel häufig nur für diese Pilotphase bereitgestellt. Wichtig ist, dass nach einer positiven Evaluierung auch weitere Mittel in den Haushalt eingestellt werden. Da nicht alle notwendigen Investitionen auf einmal getätigt werden können, sollte schrittweise vorgegangen werden, d.h., mit Blick auf die Gesamtarchitektur sollten der Einsatz von Modulen, (Teil-)Komponenten usw. eingeplant und keine statischen Zeitvorgaben ins Auge gefasst werden[36].

Der bereits erwähnten politischen Unterstützung für solche Vorhaben sollte man sich frühzeitig versichern. Darüber hinaus empfiehlt es sich schließlich, auch innerhalb der Verwaltung Mitstreiter zu suchen, die für Unterstützung sorgen, um der Gefahr zu entgehen, als Einzelkämpfer nicht ernst genommen zu werden.

Die Abstimmung mit anderen Behörden auf lokaler, Kreis-, Landes- und Bundesebene ist ein häufig vernachlässigtes eigenständiges Problemfeld. In den Fällen, in denen ein elektronischer Austausch von Informationen und Daten erfolgt, ist eine enge Abstimmung (z.B. bezüglich der verwendeten Verschlüsselungssysteme) notwendig. Dies erfordert erhebliche Kooperationsbereitschaft aller Beteiligten und bedarf wahrscheinlich umfassender Abstimmungsprozesse. Bei den Überlegungen für eine Gesamtarchitektur des IuK-Einsatzes sollte der personelle sowie technische Aufwand von vornherein mit bedacht werden.

36 Vgl. hierzu *Heinrich Reinermann*, Verwaltungsreform und technische Innovation – ein schwieriges Dauerverhältnis, in: Multimedia@Verwaltung, Jahrbuch Telekommunikation und Gesellschaft 1999, S. 11-25, hier S. 17 f.

2.3 Rechtliche Voraussetzungen [Autoren: Martin Eifert, Lutz Schreiber, Claudia Stapel-Schulz (HBI)]

In rechtlicher Hinsicht stehen den Online-Dienstleistungen der Verwaltung zwar längst nicht alle, aber zumindest wohl einige der öffentlich-rechtlichen Vorschriften entgegen, welche die Schriftform zwingend vorsehen. Daher ist es für die Umsetzung einer breiten Online-Verwaltung unumgänglich, zumindest solche verwaltungsrechtlichen Formvorschriften anzupassen. Eine Anpassung muss sich dabei vordergründig auf die Schnittstellen des Bürgers zur Verwaltung, d.h. sowohl das Antragsverfahren, als auch den Leistungsbereich der Verwaltung beziehen[37]. Dabei ist die entscheidende Frage, wie die Schriftformerfordernisse im Verwaltungsrecht zu verändern sind, um Online-Dienstleistungen der Verwaltung ohne Medienbruch gewährleisten zu können.

Außer in einigen für die *MEDIA*@Komm-Projekte nicht einschlägigen Bereichen[38] erfolgte bislang noch keine Anpassung der dem E-Government entgegenstehenden Formvorschriften des deutschen Verwaltungsrechts. Allerdings wird das Problem jetzt zunehmend angegangen.

Bremen[39] hat bereits ein Experimentalgesetz verabschiedet, das zur Erprobung der digitalen Signatur im Verwaltungsverfahren eine Übermittlung in elektronischer Form für ausgewählte Bereiche zulässt, wenn der zuständige Senator dies durch Rechtsverordnung bestimmt. Eine Rechtsverordnung in diesem Sinne wurde noch nicht erlassen. Baden-Württemberg hat einen Gesetzentwurf (e-Bürgerdienste-Gesetz) erarbeitet, der ebenfalls in ausgewählten, vom bremischen Katalog teilweise abweichenden Bereichen die Möglichkeit zum Erlass von Rechtsverordnungen eröffnet, die statt der Schriftform eine elektronische Übermittlung unter Nutzung der digitalen Signatur zulassen.

Was die Politik angeht, so gibt es Aktivitäten, um eine Überprüfung der Rechts- und Verwaltungsvorschriften des öffentlichen Rechts anzustoßen, mit dem Ziel, alternativ zur Schriftform auch die elektronische Form zuzulassen[40]. Im so genannten „Eckpunktepapier für einen Änderungsentwurf des Signaturgesetzes“[41] blieb der Handlungsbedarf für eine Anpassung der öffentlich-rechtlichen Vorschriften zwar noch unerwähnt, doch bringt jetzt das Land Baden-Württemberg einen Entschließungsantrag im Bundesrat ein, der die Bundesregierung auffordert, die Vorschriften des Bundesrechts für eine Erprobung digitaler Verwaltungsdienstleistungen anzupassen.

---

37 Vgl. dazu umfassend *Rosenbach*, Elektronische Datenverarbeitung und Verwaltungsverfahrensgesetz, Gedanken zu der Frage, inwieweit eine voll-elektronische Arbeitsweise der Verwaltung eine Gesetzesänderung erfordert, in: NWVBl 1997, S. 326 ff.

38 Beispielhaft kann § 41 der Allgemeinen Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung (SRVwV) erwähnt werden.

39 *Bremisches Gesetz zur Erprobung der digitalen Signatur in der Verwaltung*, GBl. V. 14. Juni 1999, S. 138 f.

40 Vgl. Schreiben des Bundesministeriums des Innern (BMI) an die Obersten Bundesbehörden (abgedruckt in: *Deutscher Städtetag*, Digitale Signatur auf der Basis multifunktionaler Chipkarten, 1999, S. 76 ff.).

41 Vgl. hierzu das „Eckpunktepapier“ des Bundesministeriums für Wirtschaft (BMWi) zur Änderung des Signaturgesetzes (Stand April 2000); abzurufen unter: http://www.iid.de/iukdg/gesetz/Eckpsig3.pdf.

2.4 Technische und sicherheitstechnische Voraussetzungen und Probleme [Autor: Roland Krüger (TÜViT)]

2.4.1 Einführung

2.4.1.1 Nutzung von EDV und Internet durch Verwaltungen

Noch vor wenigen Jahren waren jene Städte und Gemeinden in der kommunalen Landschaft Vorreiter, die ein Angebot im Internet bereitstellten, das wie eine Visitenkarte ein mehr oder weniger umfangreiches und qualifiziertes Informationsangebot für die Besucher der Seiten bereithielt. Neben aktuellen und umfassenden Online-Informationen im Internet werden in der (Fach-)Öffentlichkeit mittlerweile auch die Online-Kommunikation und Online-Transaktionen mit dem „elektronischen Rathaus“ diskutiert und zunehmend für selbstverständlich erachtet. So muss etwa im Verhältnis von Unternehmen und Wirtschaft zur Verwaltung einer Kommune das qualifizierte und umfassende Online-Dienstleistungsangebot als ein neuer Standortfaktor angesehen werden.

Allerdings setzt die Erweiterung der kommunalen Angebote im Netz in Richtung Kommunikation und Transaktion die Anbindung an die verwaltungsinternen Geschäftsprozesse, Datenstrukturen und die Informationstechnologie-Infrastruktur voraus. Dabei entwickelte sich die Infrastruktur aus Computern und deren Vernetzungen in den vergangenen zwanzig Jahren weder einheitlich noch strategisch geplant, sondern in Etappen am jeweiligen Bedarf und am aktuellen Stand der Technik orientiert. Dies führte zu einem Durcheinander aus verschiedenen Rechnern und Programmanwendungen: sehr viel Großrechnerarchitektur aus der Anfangszeit der Datenverarbeitung hier, eine wachsende Anzahl neuerer PC-Anwendungen dort, die nicht miteinander kommunizieren können[42].

So haben sich vor allem im letzten Jahrzehnt durch den rasanten Fortschritt bei den IuK-Technologien erhebliche Herausforderungen für die Verantwortlichen in den Kommunalverwaltungen ergeben (vgl. folgende Übersicht).

Diese technologischen Veränderungstendenzen fallen mit den Anforderungen der Kommunen im Hinblick auf das Angebot von Online-Dienstleistungen der Verwaltung zusammen und führen zu einer Vielzahl von offenen Fragen und notwendigen neuen Lösungskonzepten. So stellt sich etwa in der Verbindung der bislang abgeschlossenen informationstechnischen Systeme (behördeninternes Intranet) innerhalb eines Rathauses mit dem Internet beim Angebot bzw. die Nutzung von Kommunikations- und Transaktionsangeboten über kommunale Portale in technischer und sicherheitstechnischer Hinsicht eine Reihe von Problemen.

Für die im Rathaus bislang auch schon digitalisiert bearbeiteten und archivierten Informationen sowie die wünschenswerten Kommunikationen und Transaktionen sollen jeweils die Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit gelten, die auch sonst im Alltag an Informationsangebote, Verwaltungsverfahren, Zahlungs- und Geschäftsprozesse gestellt werden.

---

42 Aus der Pressemitteilung eines Forschungsinstituts, das mit der Analyse der IT-Infrastruktur einer Großstadtverwaltung befasst war.

Übersicht: Trends des IuK-Einsatzes in der Verwaltung*

Von ...	**... hin zu**
Großrechnern, Abteilungsrechnern	Client-/Server-Systemen
Isolierten Fachanwendungen, getrennten Großanwendungen	Verbundenen Anwendungen, integrierten Anwendungssystemen
Starren Textmasken	Graphischen, intuitiven Oberflächen
Prozeduralen Programmen	Objektorientierten Programmen
Hierarchischen Datenbanken	Relationalen Datenbanken
Eigenentwicklungen	Individuellen Anpassungen von Standardsoftware
Proprietären Systemen (Anbietermarkt)	Offenen Systemen (Käufermarkt)
Lokale, monomediale Daten	Ubiquitäre, multimediale Daten
Flickenteppich von Daten	Geordneten und abgestimmten Datenstrukturen
Angelerntem EDV-Personal	Hochqualifizierten Experten
Expertenzentrierter Softwareentwicklung	Modellierungsmethoden unter Einbeziehung von Anwendern
Anwendungssoftware mit hohem Wartungsaufwand und tendenzieller Veränderungsresistenz	Flexibel an geänderte Benutzeranforderungen angepasste IuK-Unterstützung

*Quelle: Eigene Zusammenstellung des Deutschen Instituts für Urbanistik nach *Heinrich Reinermann*, Entscheidungshilfen und Datenverarbeitung, in: Klaus König und Heinrich Siedentopf (Hrsg.), Öffentliche Verwaltung in Deutschland, Baden-Baden 1997, S. 477 – 496, hier S. 492 f.

Technik allein stellt noch kein Vertrauen her. Auch Recht allein bietet keinen realen Schutz für eine vertrauenswürdige Kommunikation. Deswegen ist Vertrauensbildung ein komplexer gesellschaftlicher Entwicklungsprozess. Die IT-Sicherheit bildet hierin einen wichtigen vertrauensbildenden Faktor.

Durch die eingesetzten IuK-Techniken sind neue Formen der Verletzlichkeit oder Verwundbarkeit der hochentwickelten Dienstleistungsgesellschaft entstanden, denn IT-Systeme können über Schwachstellen vorsätzlich und gezielt angegriffen werden. Sie sind Ziele der Wirtschafts- und Konkurrenzspionage. Gezielte Angriffe auf informationsverarbeitende Systeme können auch zur Durchsetzung von wirtschaftlichen und politischen Interessen genutzt werden.

Die Anbindung an das Internet und die weltweit voranschreitende Vernetzung der Rechner- und Computersysteme potenzieren diese Risiken. Heute ist es praktisch von jedem Punkt der Erde aus möglich, über Schwachstellen in der Informationstechnik mit mehr oder minder großem Aufwand gezielt in IT-gestützte Systeme einzudringen, diese auszuspähen, zu manipulieren, zu stören oder auszuschalten. IT-Sicherheit entwickelt sich so gesehen zu einer wichtigen wirtschaftspolitischen Herausforderung und zu einem Eckpunkt einer zukunftsorientierten Sicherheitspolitik.

Weltweit wird die IT-Sicherheit als Begriff unterschiedlich verstanden und in der Praxis oft widersprüchlich umgesetzt. Das heutige Bild ist – mit einigen lobenswerten Ausnahmen – immer noch von dem Einsatz einzelner Sicherheitsmaßnahmen geprägt, die zwar von der Verschlüsselung von Mails bis zum Einsatz von Firewalls reichen, jedoch in dieser Form (isoliert voneinander) nicht die Vorteile eines konsequenten, verwaltungsweiten Sicherheitsmanagements bieten können.

Besonders kritisch zeigt sich in der Praxis die Situation in Kommunen, die sich aus finanziellen Gründen kaum aufwendige und kostspielige Sicherheitsanalysen erlauben können. Nicht selten stellt sich hier Resignation ein, oder es werden für relativ viel Geld einzelne Sicherheitslösungen in Form von Hard- und/oder Software angeschafft, die eigentlich die viel komplexeren und zum Teil auf anderen Ebenen angesiedelten Sicherheitsprobleme der Verwaltung nicht lösen können und somit unbefriedigend wirken.

Immer noch trifft man in der Praxis auf Verantwortliche, die erst aufgrund der Jahr-2000-Diskussion oder aktueller Warnungen vor Viren wie „love-letter“ auf die IT-Sicherheitsproblematik aufmerksam geworden sind und nun gerne einiges in dieser Richtung tun würden, doch sie haben den Eindruck, damit fachlich und auch finanziell überfordert zu sein. Es fehlt der gangbare Weg. Nicht alle Bereiche sind hochsensibel. Es fehlt eine Basis, auf die Speziallösungen für einzelne, sicherheitskritische Transaktionen aufsetzen können.

2.4.1.2 Sicherheit für das vernetzte Gesamtsystem: Verwaltung – Bürger – Unternehmen

Die im Rahmen des *MEDIA*@Komm-Projekts geplanten Dienstleistungen sind oftmals Internet-Transaktionen, sodass neben der Systemsicherheit auf Seiten der Stadt und ihrer Bediensteten eine Mitverantwortung für die Systemsicherheit der Anwendung des Bürgers besteht. Der Heim-PC wird von einem Textverarbeitungs- und Informationsgewinnwerkzeug zu einem Instrument für verbindliche und reale Geschäftsprozesse. Es entstehen höhere und zum Teil neue Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit der Transaktionen bzw. Transaktionsdaten. Als Beispiel seien hier E-Commerce-Anwendungen genannt, bei denen diese neuen Anforderungen häufig auf den Bezahlvorgang (z.B. Überweisung) verlagert werden, wobei es dann leider zu einem unerwünschten Medienbruch kommt. Innerhalb des *MEDIA*@Komm-Projekts sind solche Medienbrüche gerade zu vermeiden, trotzdem sind sichere und rechtsverbindliche Willenserklärungen und Vertragsübertragungen über das Internet erforderlich. Leider ist das Internet ein sehr unsicheres Übertragungsmedium. Die Übertragungswege sind nicht kontrollierbar und werden dynamisch gebildet. Die eingesetzten Protokolle besitzen zwar Sicherungsmechanismen gegen zufällige Übertragungsfehler, nicht aber gegen Abhören und bewusste Manipulationen. Während es einer Behörde durch Firewalltechniken und einheitliche Administration der Arbeitsplätze durch Fachkräfte gelingen kann, sich gegen Angriffe aus dem Internet zu schützen, ist dies für den Bürger sehr schwierig. Zum einen fehlt es dem Bürger im Allgemeinen am notwendigen Fachwissen, zum anderen an einer geeigneten Betriebssystem-Plattform. Wie kann nun der Bürger darauf vertrauen, dass er sich im Internet hinreichend sicher bewegt, d.h. auf vertrauenswürdigen und authentischen Internetseiten mit vertrauenswürdigen und authentischen Inhalten befindet? Die hier auftauchenden möglichen Sicherheitsprobleme, seien es Viren oder unerlaubte

Zugriffe auf den Heim-PC, sind nicht allein vom Bürger beherrschbar, hier bedarf es einer Unterstützung durch den Dienstanbieter. Die Default-Einstellungen der Standard-Browser sind leider nicht auf die Systemsicherheit ausgelegt, vielmehr auf die Verfügbarkeit und Darstellung möglichst vieler Internetseiten. Beispielhaft für potenziell gefährliche Einstellungen sei hier das Zulassen aktiver Inhalte genannt, die auf fast jeder Internetseite über Script-Sprachen eingesetzt werden. Als erster Lösungsansatz können die so genannten Sandboxen bzw. die Einschränkung des Ressourcenzugriffs über Betriebssystemmittel eingesetzt werden. Leider sind solche Einschränkungen für den Bürger im Allgemeinen nicht konfigurierbar, zumal als weiteres Sicherheitsproblem in der Regel die Betriebssystemplattformen Windows 95 bzw. Windows 98 eingesetzt werden, die hierfür keine Unterstützung anbieten.

Dieses Beispiel zeigt, dass in einem Sicherheitskonzept für das „elektronische Rathaus“ neben der Systemsicherheit beim Dienstanbieter auch die Systemsicherheit beim Bürger beachtet werden muss.

Festzuhalten bleibt, dass technische und sicherheitstechnische Problemstellungen erörtert und geklärt werden sollten, bevor das „elektronische Rathaus“ durch eine Kommune realisiert werden kann. Um zu diesen Fragen eine grundlegende Orientierung zu ermöglichen, wird im Folgenden das abgestufte System sicherheitstechnischer Anforderungen und Prüfungen für IT-Systeme, wie sie sowohl im E-Commerce-Bereich, aber auch für das „elektronische Rathaus“ durchgeführt werden (sollten), dargestellt.

2.4.2 Sicherheitskonzept für IT-Systeme

2.4.2.1 Analyse

Grundsätzlich gilt, dass ein Sicherheitskonzept die Maßnahmen zur Wahrung der Informationssicherheit abdeckt. Hierzu zählen die Sicherheitspolitiken, Praktiken, Verfahren, Organisationsstrukturen und technischen Maßnahmen (Hardware/Software). Diese Maßnahmen sind zur Erfüllung der spezifischen Sicherheitsziele festzulegen. Es ist entscheidend, die Sicherheitsanforderungen zu identifizieren. Bei der Identifikation spielen drei wesentliche Aspekte eine Rolle:

1. Risiken identifizieren

   Eine Risikoanalyse ermöglicht die Identifikation von Bedrohung für die Werte, die Bewertung der Schwachstellen und der Wahrscheinlichkeit des Auftretens eines Risikos sowie die Analyse der möglichen Auswirkungen.

2. Rechtliche Aspekte beachten

   Hierunter sind Anforderungen zu verstehen, die sich aus Gesetzen (z.B. Datenschutz, SigG/SigV), Politik, Richtlinien und Verträgen ergeben, die – einschließlich der Dienstanbieter (z.B. Service Provider) – erfüllt werden müssen.

3. Informationsverarbeitung

   Dies betrifft die spezifischen Prinzipien, Ziele und Anforderungen der Informationsverarbeitung, die zur Unterstützung der Workflow-Prozesse entwickelt wurden.

Sicherheitsanforderungen werden durch eine methodische Analyse der Sicherheitsrisiken identifiziert. Der Aufwand der Maßnahmen muss gegenüber dem wirtschaftlichen und rechtlichen Schaden, der sich aus Sicherheitsversagen ergibt, abgewogen werden. Die Ergebnisse dieser Analyse unterstützen die Bestimmung von angemessenen Aktionen, Prioritäten bei der Verwaltung von Informationssicherheitsrisiken und Implementierungen der zum Schutz gegen diese Risiken ausgewählten Maßnahmen. Grundlegende Informationen über Maßnahmen bietet z.B. das IT-Grundschutz-Handbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Grundsätzlich gilt: Die im IT-Grundschutzhandbuch aufgelisteten Maßnahmen definieren eine Mindestanforderung an die IT-Sicherheit, die als Grundlage dienen kann. Der Vorteil dieses Maßnahmenkatalogs ist die umfassende Basisrealisierung von Maßnahmen zur IT-Sicherheit. Werden diese Maßnahmen erfüllt, so können hierauf aufbauend IT-Sicherheitsmaßnahmen definiert werden, die für besonders sensible Bereiche einen hohen Schutz bieten. Diese sensiblen Bereiche sind in der angesprochenen Risikoanalyse zu identifizieren, wobei auch gesetzliche Anforderungen zu berücksichtigen sind. Anwendungen, die digitale Signaturen betreffen, sind nach SigG/SigV grundsätzlich im Bereich eines hohen Schutzbedarfs anzusiedeln. Auch hier ist ein Grundschutz sinnvoll, der geeignet ergänzt wird.

2.4.2.2 Weitere Anforderungen an Sicherheitskonzepte

Um die Sicherheit durch ein Sicherheitskonzept aufrechterhalten zu können, muss das Sicherheitskonzept regelmäßig an die Anforderungen und Entwicklungen angepasst werden. Hierbei müssen die Anpassung einer Bewertung unterzogen und die Umsetzung überprüft werden.

Um den Bereich Informationssicherheit überschaubar zu machen, kann man ihn beispielsweise in eine eigene Infrastruktur einbetten. Diese Infrastruktur besteht aus einem Managementforum, das Verantwortungen an Management-Teams vergibt. Diese wiederum haben spezielle Aufgaben, bei denen sie als Ansprechpartner für sicherheitstechnische Belange dienen oder aber Maßnahmen zur Informationssicherheit in Abstimmung mit betreffenden Teams einleiten und durchsetzen.

Dies wirft folgerichtig die Frage der personellen Sicherheit auf. Deren Ziel muss es sein, dass die Risiken durch menschlichen Irrtum reduziert werden und Diebstahl, Betrug oder Missbrauch der Einrichtung verhindert werden. Dies kann durch entsprechende Arbeitsverträge und Vertraulichkeitsvereinbarungen mit den Sicherheitsverantwortlichen erreicht werden. Gleichzeitig sollte eine Überprüfung dieser Personen stattfinden.

Ein weiterer wichtiger Aspekt ist das Verhalten bei Sicherheitsvorfällen und Störungen der Informationssysteme. Die sicherheitsrelevanten Vorfälle müssen über entsprechende Managementkanäle gemeldet werden. Dies setzt voraus, dass alle Angestellten und Auftragnehmer mit dem Meldeverfahren für die verschiedenen Arten von Vorfällen (Sicherheitsverstoß, Bedrohung, Schwachstelle oder Störung), die Auswirkungen auf die Sicherheit der organisationseigenen Werte haben könnten, vertraut gemacht werden.

Die sicherheitssensiblen informationstechnischen Systeme müssen zudem an physikalisch sicheren Orten aufgestellt werden. Damit werden der unberechtigte Zugang, Be-

schädigung und Störung der Geschäftsräume und Information verhindert. Der Schutz sollte den festgestellten Risiken (Risikoanalyse) angemessen sein.

Weiterhin müssen die Benutzer der Informationssysteme geschult werden. Dies sollte gewährleisten, dass Benutzer sich der Bedrohung und Bedenken bezüglich der Informationssicherheit bewusst sind, und dass sie bei ihrer normalen Arbeitsverrichtung über Mittel zur Unterstützung der organisationseigenen Sicherheitspolitik verfügen. Überdies müssen Strategien hinsichtlich der Verfügbarkeit der angebotenen Dienste in das Gesamtkonzept integriert werden.

Einen wesentlichen Betrachtungsgegenstand innerhalb des Sicherheitskonzepts bildet die Rolle der Zertifizierungs- und Registrierungsstellen. Wird auf bestätigte Stellen zurückgegriffen, so können die bei der Bestätigung dieser Stellen vorgelegten Konzepte integriert werden, ansonsten sind eigene Konzeptlösungen zu qualifizieren und zu bestätigen. Die Sicherheit des Gesamtverfahrens muss aufrechterhalten bleiben, d.h. Verschlüsselung, digitale Signaturen und die Infrastruktur müssen im Zusammenhang betrachtet werden – und sind auch nur im Zusammenspiel wirksam.

Nach diesen allgemeinen Ausführungen zu Sicherheitskonzepten und damit zusammenhängenden Anforderungen an IT-Systeme soll im Folgenden zunächst der schon oben erwähnte IT-Grundschutz näher erläutert werden. Im Hinblick auf Online-Dienstleitungen der Verwaltung ist der IT-Grundschutz als Voraussetzung für die zugrunde liegenden IT-Systeme anzusehen. Für spezielle Angebote des „elektronischen Rathauses“ – insbesondere Kommunikations- und Transaktionsmöglichkeiten unter Nutzung der digitalen Signatur – ist darüber hinausgehenden Anforderungen im Hinblick auf die einzelnen Komponenten und deren Zusammenspiel in einem IT-Gesamtsystem gerecht zu werden. Hier sind nach SigG/SigV unter Umständen Risikoanalysen, Evaluation bzw. Bestätigung für Komponenten sowie Prozesse in einem Gesamtsystem von akkreditierten Prüfinstanzen erforderlich.

2.4.3 Exkurs: Einführung in den IT-Grundschutz

2.4.3.1 Hintergrund

Die Bundesverwaltung ist seit Jahren gehalten, im Zusammenhang mit IT-Rahmenkonzepten auch IT-Sicherheitskonzepte zu erstellen. Anfänglich wurden diese IT-Sicherheitskonzepte anhand einer aufwendigen Risikoanalyse, zum Beispiel nach dem IT-Sicherheitshandbuch, erstellt. Zur Reduzierung des Aufwands und zur Optimierung der Ergebnisse wurden begleitende Schulungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) durchgeführt und Vereinfachungsansätze zur Risikoanalyse veröffentlicht.

Die Vielzahl und Vielfalt der Behörden, die ein IT-Sicherheitskonzept erstellen müssen, stellt einen repräsentativen Querschnitt von IT-Anwendern dar, aus dem man ableiten kann, dass effektive und aussagekräftige IT-Sicherheitskonzepte auf Basis von Risikoanalysen praktisch nur von erfahrenen IT-Sicherheitsfachleuten erstellt werden können. Vor diesem Hintergrund wurde versucht, die Erstellung von IT-Sicherheits-

konzepten zu vereinfachen, ohne deren Qualität einzuschränken. Die Idee des IT-Grundschutzes war geboren.

Der Aufwand für IT-Sicherheitskonzepte sollte auf die hochschutzbedürftigen IT-Systeme konzentriert werden, indem für mittelschutzbedürftige IT-Systeme ein standardisiertes Verfahren, eben der IT-Grundschutz, eingesetzt wird.

2.4.3.2 Ziel des IT-Grundschutzes

Ziel des IT-Grundschutzes ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den mittleren Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Anwendungen dienen kann. Derartige

- infrastrukturelle
- organisatorische
- personelle und
- technische

IT-Sicherheitsmaßnahmen für eine Reihe von typischen IT-Systemen und Einsatzumgebungen werden in einem Regelwerk gebündelt.

Damit muss der Anwender des entsprechenden Regelwerks nur noch einen Soll-Ist-Vergleich durchführen, um fehlende IT-Sicherheitsmaßnahmen zu identifizieren. Da für jede einzelne Maßnahme auch Realisierungsvorschläge ausgearbeitet wurden, ist die Umsetzung der IT-Grundschutzmaßnahmen kurzfristig möglich, zumal kostspielige Maßnahmen für den mittleren Schutzbedarf kaum benötigt werden.

IT-Grundschutz wird somit zu einer gemeinsamen Verständigungsbasis im Hinblick auf Maßnahmen für den mittleren Schutzbedarf.

2.4.3.3 Grenzen des IT-Grundschutzes

Die für den IT-Grundschutz statthaften pauschalen Ansätze von Maßnahmenempfehlungen reichen jedoch nicht ohne weiteres für hochschutzbedürftige IT-Systeme aus. Systeme geringeren Schutzbedarfs sind häufig solche Systeme, die reinen Informationscharakter besitzen, eventuell auch eine Kommunikation über Rückmeldungen erlauben. Sensible Bereiche stellen z.B. Transaktionen dar, wie sie typischerweise bei E.Commerce oder im Umfeld digitaler Signaturen auftreten.

In solchen Fällen können individuelle Sicherheitsuntersuchungen detaillierte Ergebnisse erzielen, insbesondere bei der Auswahl geeigneter Sicherheitsmaßnahmen unter Beachtung von Kosten- und Wirksamkeitsaspekten. Entsprechende Analysen sind in der Lage, über die IT-Grundschutzmaßnahmen hinaus zusätzliche oder qualitativ wirksamere Maßnahmen herauszuarbeiten. Grundsätzlich ist es geboten, bei hochschutzbedürftigen IT-Anwendungen neben der Realisierung des IT-Grundschutzes auf individuelle Sicherheitsuntersuchungen nicht zu verzichten.

2.4.3.4 Dynamik des IT-Sicherheitsprozesses

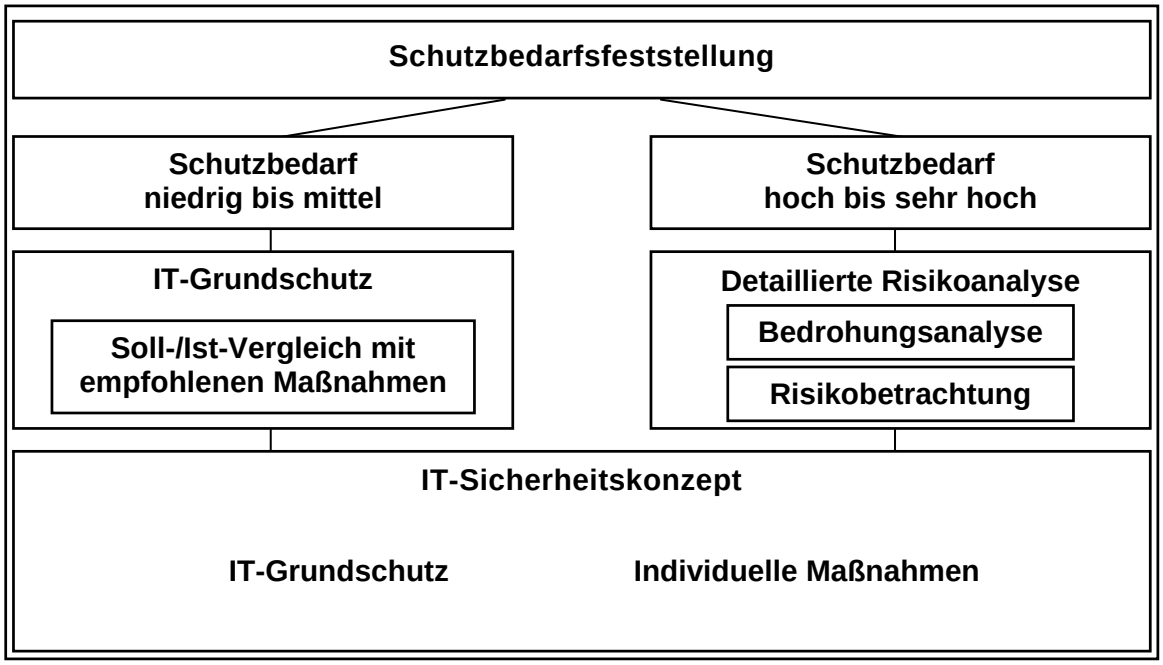
Das einmalige Erstellen eines IT-Sicherheitskonzepts, auch auf der Basis von IT-Grundschutz-Betrachtungen, ist für eine umfassende IT-Sicherheit nicht ausreichend. Vielmehr ist es erforderlich, den IT-Sicherheitsprozess durch einen Regelkreislauf aus Konzeption, Realisierung und Kontrolle von IT-Sicherheitsmaßnahmen zu gestalten.

Diese Aufgabe ist von fundamentaler Bedeutung und muss durch den Dienstanbieter initiiert werden.

2.4.3.5 Schutzbedarfsfeststellung

Entscheidend für die Anwendbarkeit unterschiedlicher Strategien ist eine vorab durchzuführende Schutzbedarfsfeststellung, um so die Bereiche zu identifizieren, in denen ein IT-Grundschutz vollkommen ausreicht und auf aufwendige Risikoanalysen verzichtet werden kann. Die Methode IT-Grundschutz ist nicht geeignet für Risikoanalysen, insbesondere nicht für Risikoanalysen in sicherheitstechnisch sensiblen Bereichen. Das Ziel der Methode ist letztlich die Vermeidung solcher Analysen für den mittleren Schutzbedarf.

Übersicht: Schutzbedarfsfeststellung*



*Quelle: Eigene Ausarbeitung.

Je stärker das Bedrohungsbild von den Standard-Bedrohungen abweicht, desto größer wird der individuelle Schutzbedarf. Zur Deckung dieses erhöhten Bedarfs (E-Commerce, Online-Dienstleistungen der Verwaltung unter Nutzung der Digitalen Signatur gegebenenfalls mit oder ohne Payment) existieren Firmen, die durch weitere Maßnahmen (Sicherheitsanalysen, sicherheitstechnische Qualifizierungen, Prüfungen, Validierungen, Evaluationen usw.) anderen Sicherheitsrisiken vorbeugen, Risiken diagnostizieren und auch Lösungen anbieten.

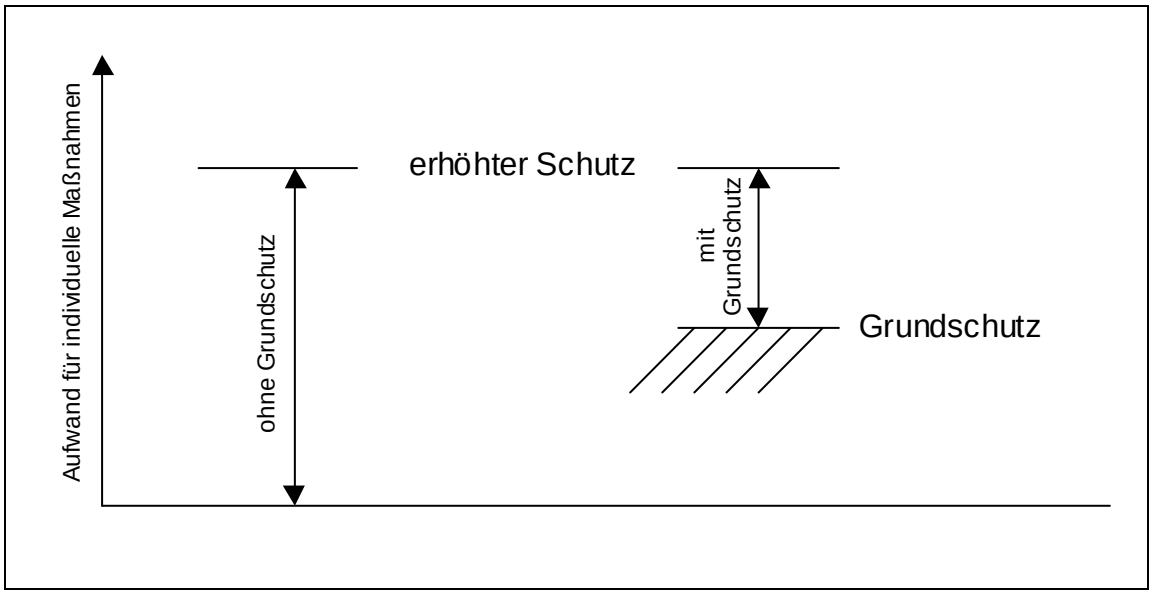
Neben der präventiven Funktion hat der IT-Grundschutz außerdem einen wichtigen Nebeneffekt: die Erhöhung der Effektivität und insbesondere der Wirtschaftlichkeit der IT-Sicherheit. Denn es ist umso leichter, sicherer und auch wirtschaftlicher, individuelle Sicherheitsmaßnahmen festzulegen, je besser und stabiler der Grundschutz funktioniert. So empfiehlt sich der IT-Grundschutz als wesentlicher Grundbaustein für jede Security-Initiative mit System.

2.4.3.6 Kunden-Nutzenargumentation

In der Bestimmung des IT-Sicherheitsniveaus für eine Kommune spielt das Kosten/Nutzen-Verhältnis eine entscheidende Rolle. Es ist hier wichtig zu beachten, dass das gewählte Schutzniveau des IT-Systems zur Realisierung des „elektronischen Rathauses“ nur mit einem entsprechenden Aufwand zu erreichen ist.

Das nachstehende Diagramm soll verdeutlichen, wieviel Aufwand in Relation zu dem angestrebten IT-Sicherheitsniveau zu betreiben ist. Dieser Aufwand bietet eine Orientierung für die personellen, zeitlichen und finanziellen Ressourcen, die zur Realisierung der IT-Sicherheitsziele notwendig sind.

Abbildung: Relation von Aufwand und IT-Sicherheitsniveau



*Quelle: Eigene Ausarbeitung.

Aus dem Diagramm ist zu entnehmen, dass die Implementierung von Grundschutz-Maßnahmen ein hervorragendes Kosten-Nutzen-Verhältnis bietet. Da, wo reine Information bzw. auch Kommunikation eine Rolle spielen, reicht der IT-Grundschutz in der Regel vollkommen aus. Für sensible Bereiche des E-Commerce oder der Anwendung der digitalen Signatur muss aber stets im Einzelfall überprüft werden, ob hier – insbesondere bei Transaktionen – der IT-Grundschutz ausreicht, zumal auch durch das Signaturgesetz ein hoher Schutzbedarf bei der digitalen Signatur festgeschrieben ist.

2.4.4 Anforderungen an technische Komponenten für Online-Dienstleistungen der Verwaltung unter Nutzung der digitalen Signatur

Der IT-Grundschutz reicht für IT-Systeme, die Konzepte von „elektronischen Rathäusern“ mit umfassenden Kommunikations- und vor allem Transaktionsangeboten (mit/ohne Payment) realisierbar machen sollen, nicht aus. Durch die Verwendung digitaler Signaturen bestehen nach SigG/SigV Anforderungen an die technischen Komponenten zur Erzeugung und Prüfung solcher Signaturen wie auch an die Sicherheit der Gesamtlösung. Betrachtet man die Einzelkomponenten im Umfeld digitaler Signaturen, so sind nach SigG/SigV bestätigte Komponenten einzusetzen. Eine solche Bestätigung umfasst eine erfolgreiche Evaluation dieser Komponenten nach ITSEC, hier nach den Stufen *E2 hoch* bzw. *E4 hoch*.

Als technische Komponenten sind hier insbesondere zu nennen:

- Personalisierte Chipkarten (Schlüsselerzeugung in einer Zertifizierungsstelle oder direkt auf der Chipkarte): Evaluation nach ITSEC *E4 hoch* zuzüglich der Bestätigung nach SigG/SigV;
- Komponenten zur Signaturerstellung sowie Prüfung von Signaturen und Zertifikaten, einschließlich der Darstellungskomponente;
- private Nutzung (z.B. privater PC): Evaluation nach ITSEC *E2 hoch* zuzüglich der Bestätigung nach SigG/SigV;
- gewerbliche Nutzung (z.B. Kioskbetrieb): Evaluation nach ITSEC *E4 hoch* zuzüglich der Bestätigung nach SigG/SigV.

Für weitere Komponenten, so z.B. entsprechende TV- oder Handykomponenten, ist für die notwendige Evaluationsstufe die gedachte Einsatzumgebung entscheidend: Bei rein privater Nutzung reicht die ITSEC-Evaluationsstufe *E2 hoch* aus (z.B. Handy oder TV im Heimbereich), bei auch öffentlich genutzten Komponenten (z.B. TV im Eingangsbereich einer Behörde) ist aber eine Evaluation und Bestätigung gemäß ITSEC *E4 hoch* erforderlich.

Man beachte: Die Anforderung, einzelne Komponenten nach ITSEC evaluieren zu lassen, entstammt zum einen gesetzlichen Auflagen (SigG/SigV), zum anderen kann eine solche Anforderung als Analyseergebnis aus dem Sicherheitskonzept stammen: Für bestimmte Bereiche werden besondere Anforderungen an die IT-Sicherheit der eingesetzten Produkte gestellt. Ob ein Produkt diese erfüllt, kann auf verschiedene Arten verifiziert werden. Einerseits kann man einem Werbeprospekt oder der Herstelleraussage, andererseits dem Prüfergebnis eines unabhängigen Dritten vertrauen, der ein solches Produkt nach anerkannten Kriterien (z.B. ITSEC) überprüft (evaluiert). Wichtig ist festzuhalten: Nicht alle Bereiche sind hochschutzbedürftig. Entscheidend ist die Sicherheit des Gesamtsystems. Dessen Überprüfung erfolgt jedoch nicht durch eine Evaluation, da solche Verfahren für komplexe Systeme zu aufwendig sind. Hier sollte auf Alternativen wie eine sicherheitstechnische Qualifizierung zurückgegriffen werden. Mit solchen Methoden kann das Zusammenwirken einzelner Systeme überprüft werden. Ob die Einzelsysteme vertrauenswürdig sind, muss individuell entschieden werden. Neben der Überprüfung einzelner System (Evaluation) muss zudem deren korrekte

Konfiguration und Einbettung in den Gesamtablauf betrachtet werden. Eine solche Überprüfung der Gesamtsicherheit geschieht im Rahmen der Abnahme des Sicherheitskonzepts. Das Sicherheitskonzept kann sich hierbei auf bestätigte Einzelkomponenten abstützen. Der folgende Exkurs dient dazu, den Prozess einer Evaluation von Einzelkomponenten darzulegen.

2.4.4.1 Exkurs Einführung in die ITSEC

Unter der Abkürzung ITSEC versteht man die europäisch harmonisierten Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik, genauer: Information Technology Security Evaluation Criteria, Harmonised Criteria of France, Germany, the Netherlands, the United Kingdom, Version 1.2 vom 28. Juni 1991.

Wie auch die deutschen IT-Sicherheitskriterien gehen die ITSEC von drei Grundbedrohungen aus: Verlust von Vertraulichkeit, Integrität und Verfügbarkeit. Diesen Bedrohungen soll mit einer vertrauenswürdigen Implementation von Sicherheitsfunktionen entgegengewirkt werden. Am Anfang des Designs der Sicherheitsfunktionen muss daher eine ausführliche Bedrohungsanalyse stehen. Die ITSEC unterscheiden in diesem Zusammenhang den Begriff IT-System, das eigenständig in einer bekannten Umgebung eingesetzt werden soll und für das reale Bedrohungen bekannt sind, sowie den Begriff IT-Produkt, dessen Einsatzumgebung nicht vorhersehbar ist und für das ein fiktives Bedrohungsmodell aufgestellt werden muss. Diese Unterscheidung wird im Folgenden jedoch vernachlässigt.

Die *Evaluation* eines IT-Produkts nach den ITSEC bedeutet eine Bewertung der Vertrauenswürdigkeit der in diesem Produkt zum Zwecke der Einhaltung definierter Sicherheitsziele verwirklichten technischen Sicherheitsmaßnahmen, welche im Folgenden als *Sicherheitsfunktionen* bezeichnet werden. Unter *Vertrauenswürdigkeit* versteht man hierbei jene Eigenschaft des Produkts, die das Maß an Vertrauen in die *Korrektheit* und *Wirksamkeit* der Implementierung der angegebenen Sicherheitsfunktionen ausdrückt. Den Maßstab für die Bewertung bildet die vom Antragsteller der Evaluation vorgegebene *Evaluationsstufe* (E0, E1, E2 bis E6). Im Zusammenhang mit der Bestätigung technischer Komponenten nach SigG/SigV ergeben sich die Sicherheitsziele aus den dort definierten Anforderungen; die relevanten Evaluationsstufen sind die Stufe E4 für die technischen Komponenten, die direkt mit privaten Signaturschlüsseln operieren, und die Stufe E2 für die übrigen Komponenten nach SigG/SigV.

Neben den Evaluationstufen, die ein Maß für die Prüftiefe und somit für die Vertrauenswürdigkeit sind, wird bei einer Evaluation auch die Mechanismenstärke der eingesetzten Sicherheitsmechnismen bewertet. Die Sicherheitsmechnismen dienen zur Realisierung der Sicherheitsfunktionalität. Die Stärke der Sicherheitsmechanismen ist ihre Fähigkeit, einem direkten Angriff zu widerstehen. Die Analyse der Mechanismenstärke stützt sich auf die folgenden Aspekte: Fachkenntnisse, geheime Absprache, Zeit und Ausstattung eines potenziellen Angreifers. Nach den ITSEC-Kriterien werden die Mechanismenstärken in die Kategorien niedrig, mittel und hoch eingeteilt, wobei nach SigG/SigV eine hohe Mechanismenstärke gefordert ist, unabhängig von der Prüftiefe bzw. Evaluationsstufe.

2.4.4.1.1 Kurzcharakterisierung der Qualitätsstufen

Stufe E0:

- unzureichende Vertrauenswürdigkeit.

Stufe E1:

- Sicherheitsvorgaben[43] müssen vorliegen;
- informelle Beschreibung des Architekturentwurfs;
- funktionale Tests auf Erfüllung der Sicherheitsvorgaben.

Stufe E2 (zusätzlich zu E1):

- informelle Beschreibung des Feinentwurfs;
- Bewertung der funktionalen Tests;
- Konfigurationskontrollsystem muss vorhanden sein;
- genehmigtes Distributionsverfahren muss vorhanden sein.

Stufe E3 (zusätzlich zu E2):

- Bewertung des den Sicherheitsmechanismen entsprechenden Quellcodes;
- Bewertung der Tests der Sicherheitsmechanismen.

Stufe E4 (zusätzlich zu E3):

- formales Sicherheitsmodell (für ein BS z.B. Bell-La-Padula-Modell);
- sicherheitsspezifische Funktionen, Architekturentwurf und Feinentwurf in semiformaler Notation.

Stufe E5 (zusätzlich zu E4):

- enger Zusammenhang zwischen Feinentwurf und Quellcode.

Stufe E6 (zusätzlich zu E5):

- sicherheitsspezifische Funktionen, Architekturentwurf in formaler Notation, wobei Konsistenz zum unterliegenden Sicherheitsmodell gefordert ist.

2.4.4.1.2 Beurteilungsaspekte

Die Evaluation soll das Vertrauen in die Tatsache bewerten, dass die in einem IT-System implementierten Sicherheitsfunktionen auch das Sicherheitsziel erreichen. Da-

43 Das Dokument Sicherheitsvorgaben enthält:
1.) Systemsicherheitspolitik (oder eine Produktbeschreibung);
2.) Spezifikation der geforderten sicherheitsspezifischen Funktionen;
3.) Definition der geforderten Sicherheitsmechanismen;
4.) postulierte Mindeststärke der Mechanismen;
5.) angestrebte Evaluationsstufe.

bei werden einerseits das Vertrauen in die Korrektheit der Implementierung und andererseits das Vertrauen in die Wirksamkeit der implementierten Mechanismen beurteilt.

Letztere Prüfung gliedert sich wie auch die Prüfung der Korrektheit in zwei Life-Cycle-Phasen, nämlich die Phase der Herstellung bzw. Konstruktion und in die Betriebsphase. Bei der Wirksamkeit werden im Einzelnen folgende Aspekte betrachtet:

Wirksamkeitskriterien – Konstruktion

- Aspekt 1 – Eignung der Funktionalität
- Aspekt 2 – Zusammenwirken der Funktionalität
- Aspekt 3 – Stärke der Mechanismen
- Aspekt 4 – Konstruktionsschwachstellen

Wirksamkeitskriterien – Betrieb

- Aspekt 1 – Benutzerfreundlichkeit
- Aspekt 2 – Bewertung der operationalen Schwachstellen

Da für die Prüfung der Wirksamkeit eine Schwachstellenanalyse anzufertigen ist, die sich auf Informationen stützt, die in der Korrektheitsbewertung erarbeitet werden, wird diese Prüfung nach Darlegung der Kriterien für die einzelnen Qualitätsstufen betrachtet.

Der Korrektheitsaspekt bei der Vertrauenswürdigkeit wird formal unter folgenden Gesichtspunkten betrachtet:

Konstruktion – Entwicklungsprozess

- Phase 1 – Anforderungen
- Phase 2 – Architekturentwurf
- Phase 3 – Feinentwurf
- Phase 4 – Implementierung

Konstruktion – Entwicklungsumgebung

- Aspekt 1 – Konfigurationskontrolle
- Aspekt 2 – Programmiersprachen und Compiler
- Aspekt 3 – Sicherheit beim Entwickler

Betrieb – Betriebsdokumentation

- Aspekt 1 – Benutzerdokumentation
- Aspekt 2 – Systemverwalter-Dokumentation

Betrieb – Betriebsumgebung

- Aspekt 1 – Auslieferung und Konfiguration
- Aspekt 2 – Anlauf und Betrieb

Um zu einem vollständigen und transparenten Verständnis zu gelangen, ob das Produkt seine definierten Sicherheitsziele mit dem Grad des Vertrauens erfüllt, welcher

durch den Evaluationslevel vorgegeben ist, müssen Dokumente bezüglich der *Konstruktions-* und der *Betriebsphase* des Produkts zur Verfügung gestellt werden.

Exemplarisch wird nachfolgend die benötigte Mindestdokumentation für die Stufen E2 und E4 angegeben, da diese Evaluationsstufen nach SigG/SigV relevant sind. Hierbei werden diejenigen Anforderungen für die Stufe E4, die für E2 nicht erforderlich sind, in KAPITÄLCHEN gesetzt *und* durch eckige Klammern **[ ]** umschlossen[44].

Von dem Produkthersteller wird erwartet, dass er die unten spezifizierten Dokumente im Hinblick auf Inhalt, Form und Nachweise gemäß ITSEC, S. 62-69 bzw. S. 79-87 (Korrektheit) und S. 37-43 (Wirksamkeit) erstellt und der beauftragten Prüfstelle (Prüfstelle für IT-Sicherheit der TÜV Informationstechnik GmbH) zur Verfügung stellt. Nach einer erfolgreichen Evaluation wird durch eine Bestätigungsstelle (Bestätigungsstelle nach SigG/SigV der TÜV Informationstechnik GmbH) bestätigt, dass eine erfolgreich durchgeführte Evaluation die Sicherheitsziele nach SigG/SigV abdeckt und die technischen Komponenten somit nach SigG/SigV als bestätigte Komponenten zugelassen werden können.

2.4.4.1.3 Dokumentenforderung bezüglich Korrektheit in der Konstruktion

Sicherheitsvorgaben

Die Sicherheitsvorgaben sind das zentrale Dokument und bilden die Grundlage für alle weiteren während des Evaluationsprozesses zu erstellenden Dokumente. Sie beinhalten eine Produktbeschreibung, die die Art des Produkteinsatzes, die vorgesehene Einsatzumgebung, die zu erreichenden Sicherheitsziele und die angenommenen Bedrohungen des Produkts darlegen. Zudem sind eine Spezifikation der vom Produkt geforderten Sicherheit (Sicherheitsfunktionen), die Mindeststärke der die Sicherheitsfunktionen realisierenden *Sicherheitsmechanismen*[45] (niedrig, mittel oder hoch)[46] sowie die angestrebte Evaluationsstufe im Rahmen der Sicherheitsvorgaben anzugeben.

[FORMALES SICHERHEITSMODELL

BEI DEN EVALUATIONSSTUFEN AB E4 MUSS EIN IN FORMALER NOTATION SPEZIFIZIERTES SICHERHEITSMODELL DEFINIERT ODER EIN VERWEIS AUF EIN SOLCHES ANGEGEBEN WERDEN, WELCHES DIE VOM EVALUATIONSGEGENSTAND DURCHGESETZTE SICHERHEITSPOLITIK FESTLEGT. ES MUSS GEZEIGT WERDEN, DASS DIE SICHERHEITSVORGABEN DIE ZUGRUNDE LIEGENDE SICHERHEITSPOLITIK UMSETZEN UND KEINE FUNKTIONEN ENTHALTEN, DIE ZU DIESER POLITIK IM WIDERSPRUCH STEHEN.**]**

---

44 Zum Erreichen der Stufe E4 ist aber insgesamt sowohl ein höherer Granularitätsgrad bezüglich der einzelnen Nachweise als auch die Verwendung einer *semiformalen Notation* in den Dokumenten *Sicherheitsvorgaben*, *Architektur-* und *Feinentwurf* obligat.

45 Die Logik/der Algorithmus, die/der eine bestimmte sicherheitsspezifische oder -relevante Funktion in Hard- oder Software implementiert.

46 Gemäß ITSEC, Abschnitt 3.6-3.8 bedeutet *niedrig:* Schutz vor Bedienungsfehlern, *mittel:* Schutz vor Benutzern mit beschränkten Hilfsmitteln, *hoch:* Schutz vor Anwendern mit sehr guten Fachkenntnissen und Hilfsmitteln.

Architekturentwurf

Der Architekturentwurf stellt zusammen mit dem nachfolgenden Feinentwurf die für die Evaluation notwendige Designbeschreibung dar. Architektur- und Feinentwurf ergänzen einander und bilden zwei Ebenen der Beschreibungshierarchie. Der Architekturentwurf ist die obere Ebene, die über eine Top-Level-Zuordnung abstrakter Funktionen zu logischen und physischen Komponenten verdeutlicht, wie die in den Sicherheitsvorgaben festgelegten Sicherheitsfunktionen zur Verfügung gestellt werden.

Feinentwurf

Der Feinentwurf stellt eine Verfeinerung der Architekturbeschreibung dar, in der die Funktionalität der einzelnen Komponenten sichtbar wird. Die Beschreibung erfolgt dabei bis hin zu einem Detaillierungsgrad, der als Basis für die Programmierung und/oder Hardware-Konstruktion verwendet werden kann. Der Feinentwurf expliziert über die Spezifikation von Sicherheitsmechanismen, auf welche Weise die Sicherheitsfunktionen realisiert werden.

Testdokumentation

Die Testdokumentation ist das Mittel zur Überprüfung der Implementierung des Feinentwurfs auf Übereinstimmung mit den Sicherheitsvorgaben. Sie beinhaltet neben Testplänen, -zielen, -verfahren und -ergebnissen auch die Bibliothek der Testprogramme und -werkzeuge, die für die Tests benutzt wurden.

[QUELLCODE/HW-KONSTRUKTIONSZEICHNUNGEN

FÜR ALLE *SICHERHEITSSPEZIFISCHEN* UND *-RELEVANTEN* KOMPONENTEN[47] MÜSSEN DER QUELLCODE BZW. DIE HW-KONSTRUKTIONSZEICHNUNGEN SOWIE EINE ZUORDNUNGSBESCHREIBUNG, DIE DEN BEZUG ZWISCHEN QUELLCODE/HARDWARE-KONSTRUKTIONSZEICHNUNGEN UND DEM FEINENTWURF DARSTELLT, ZUR VERFÜGUNG GESTELLT WERDEN.**]**

Konfigurationsliste

Die Konfigurationsliste identifiziert eindeutig das Produkt (Version), seine Komponenten und alle für die Evaluation zur Verfügung gestellten Dokumente.

Konfigurationskontrolle

Dieses Dokument gibt Informationen über das **[**DURCH WERKZEUGE UNTERSTÜTZTE**]** *Konfigurationskontrollsystem*, d. h. die Kontrollen, die der Entwickler des Produkts hinsichtlich seiner Entwicklungs-, Produktions- und Wartungsprozesse durchgeführt hat, und wie das Konfigurationskontrollsystem im Entwicklungsprozess zusammen mit dem Qualitätsmanagementverfahren angewendet wird.

47 Sicherheitsspezifisch: Das, was unmittelbar zur Sicherheit beiträgt. Sicherheitsrelevant: Das, was nicht sicherheitsspezifisch ist, jedoch korrekt funktionieren muss, damit der Evaluationsgegenstand die Sicherheit garantieren kann.

[ZUSÄTZLICH MUSS DER ENTWICKLUNGSVORGANG DURCH EIN ABNAHMEVERFAHREN UNTERSTÜTZT SEIN, WELCHES OBJEKTE, DIE WÄHREND DES ENTWICKLUNGS-, PRODUKTIONS- UND WARTUNGSPROZESSES ERSTELLT WURDEN, EINDEUTIG IN EIN KONFIGURATIONSKONTROLLSYSTEM ZUR KONTROLLE EINBEZIEHT.**]**

[PROGRAMMIERSPRACHEN UND COMPILER

IN DIESEM DOKUMENT SIND SÄMTLICHE FÜR DIE IMPLEMENTIERUNG BENUTZTEN PROGRAMMIERSPRACHEN UND IMPLEMENTIERUNGSABHÄNGIGEN OPTIONEN DER PROGRAMMIERSPRACHEN KLAR DEFINIERT. ZUDEM SIND FÜR ALLE BENUTZTEN COMPILER DIE GEWÄHLTEN IMPLEMENTIERUNGSOPTIONEN DOKUMENTIERT.**]**

Sicherheit beim Entwickler

Dieses Dokument verdeutlicht über die Beschreibung materieller, organisatorischer, personeller und anderer Sicherheitsmaßnahmen, dass aus der Herkunft des Produkts keine Gefahren zu befürchten sind. Es zeigt, wie die Integrität des Produkts und die Vertraulichkeit der zugehörigen Dokumente gewährleistet werden.

2.4.4.1.4 Dokumentenforderung bezüglich Korrektheit im Betrieb

Benutzer- und Systemverwalterdokumentation

Die Dokumente stellen sicher, dass alle Benutzer und mit Privilegien ausgestattete Systembediener und -verwalter über die sicherheitsrelevanten Aspekte umfassend, verständlich und eindeutig informiert sind, um das Produkt sicher benutzen und verwalten zu können.

Auslieferungs- und Konfigurations-Dokumentation

Diese Dokumente verdeutlichen, wie die Sicherheit während des Transports des Produkts oder seiner Komponenten zum Anwender hinsichtlich der Erstauslieferung und auch hinsichtlich später folgender Modifikationen gewahrt bleibt. Dazu muss ein für diese Stufe vom BSI[48] zugelassenes Verfahren Anwendung finden.

Anlauf- und Betriebs-Dokumentation

Die Dokumente geben Informationen, wie die Sicherheit des Produkts während des Anlaufs und des Betriebs aufrechterhalten bleibt. Die Verfahren, die beispielsweise ein Systemverwalter zum sicheren täglichen Betrieb des Produkts benutzt, sind hier darzulegen. **[**VERFAHREN MÜSSEN VORHANDEN SEIN, DIE DEN EVALUATIONSGEGENSTAND NACH EINEM SYSTEMAUSFALL ODER NACH EINEM HARD- ODER SOFTWAREFEHLER IN EINEN SICHEREN ZUSTAND ZURÜCKVERSETZEN KÖNNEN.**]**

48 Bundesamt für Sicherheit in der Informationstechnik, Sitz in Bonn.

2.4.4.1.5 Dokumentenforderung bezüglich Wirksamkeit in der Konstruktion

Analyse der Eignung

Dieses Dokument analysiert die Eignung der Sicherheitsfunktionen, den in den Sicherheitsvorgaben zitierten Bedrohungen entgegenzuwirken. Die Analyse muss zeigen, dass und auf welche Art allen identifizierten Bedrohungen durch die Sicherheitsfunktionen begegnet wird.

Analyse des Zusammenwirkens

Dieses Dokument analysiert die Fähigkeit der Sicherheitsfunktionen und der sie realisierenden Mechanismen, in einer Weise zusammenzuwirken, dass sie sich gegenseitig unterstützen (Synergieeffekte). Die Analyse muss zeigen, dass die Gesamtheit der Sicherheitsfunktionen zusammen mit der Beschreibung ihres Zusammenwirkens entsprechend den Angaben des Architekturentwurfs die Gesamtheit der Sicherheitsziele erfüllt, d.h. alle in den Sicherheitsvorgaben aufgeführten Bedrohungen abdeckt.

Analyse der Stärke der Mechanismen

Dieses Dokument analysiert die Fähigkeit der Sicherheitsmechanismen, einem direkten Angriff zu widerstehen. Die Analyse stützt sich bei der Bewertung der Stärke der Mechanismen auf die folgenden Aspekte: Fachkenntnisse, geheime Absprache, Zeit und Ausstattung eines potenziellen Angreifers. Nach den ITSEC-Kriterien werden die Mechanismenstärken in die Kategorien niedrig, mittel und hoch eingeteilt, wobei nach SigG/SigV eine hohe Mechanismenstärke gefordert ist, unabhängig von der Prüftiefe bzw. Evaluationsstufe.

Liste der bekannten Schwachstellen in der Konstruktion

Dieses Dokument analysiert die Auswirkungen jeder bekannten *Konstruktionsschwachstelle*, d.h. Schwachstellen, die irgendeine während der Konstruktion eingebrachte Eigenschaft des Evaluationsgegenstands ausnutzen. Es müssen Maßnahmen zur Abhilfe aufgezeigt werden, sodass in der definierten Einsatzumgebung die Sicherheit des Produkts nicht kompromittiert werden kann.

2.4.4.1.6 Dokumentenforderung bezüglich Wirksamkeit im Betrieb

Analyse der Benutzerfreundlichkeit

Bei diesem Aspekt der Wirksamkeit wird geprüft, ob der Evaluationsgegenstand in einer Weise konfiguriert oder genutzt werden kann, die unsicher ist, die aber von einem Systemverwalter oder Endanwender berechtigterweise für sicher gehalten würde.

Liste der bekannten Schwachstellen in der operationellen Nutzung

Dieses Dokument analysiert die Auswirkungen jeder bekannten *Schwachstelle im Betrieb*, d.h. Schwachstellen, die Schwächen nichttechnischer Gegenmaßnahmen ausnutzen, um die Sicherheit des Evaluationsgegenstands zu verletzen. Es müssen Maßnahmen zur Abhilfe aufgezeigt werden, sodass in der definierten Einsatzumgebung die Sicherheit des Produkts nicht kompromittiert werden kann.

Nach diesem Exkurs wird deutlich, dass der Aufwand für die nach SigG/SigV verbindliche Evaluation und Bestätigung der technischen Komponenten leicht unterschätzt wird, sodass gegebenenfalls auf bereits evaluierte und bestätigte Komponenten zurückgegriffen werden sollte. Auf diese Komponenten kann dann eine technische Plattform zurückgreifen, die das beabsichtigte Dienstangebot bereitstellt. Eine solche Plattform ist in ein Sicherheitskonzept einzubetten, um die Sicherheit der Gesamtlösung gewährleisten zu können. Ein nahe liegender Gedanke hinsichtlich der technischen Plattformen und der einzelnen technischen Komponenten ist der Versuch der Nutzung bzw. Übertragbarkeit von bereits entwickelten Lösungen aus dem E-Commerce-Bereich. Ließen sich derartige Lösungen ohne größere Schwierigkeiten übertragen, dann könnten insgesamt sicherlich in erheblichem Maße Ressourcen gespart werden. Technische Plattformen aus dem E-Commerce-Bereich sind im Allgemeinen zwar fähig, digitale Signaturen auszustellen und zu prüfen, sie sind aber keine generell nach SigG/SigV bestätigten Komponenten, sodass auch vor dem Hintergrund von SigG/SigV Erweiterungen notwendig werden können. Zumindest sind entsprechende Bestätigungen der technischen Komponenten beizubringen. Neben den Anforderungen von SigG/SigV bestehen noch weitere Anforderungen, z.B. aus dem Bereich des Datenschutzes und der Verfügbarkeit angebotener Dienste. E-Commerce-Lösungen erfüllen zwar auch gewisse Anforderungen an den Datenschutz, insbesondere bei der Übertragung von Kunden zur Bank. Allerdings sind Datenschutzaspekte innerhalb von Banken einschließlich der Mitarbeiter häufig nicht relevant. Innerhalb der Städte stellt sich diese Situation oft deutlich anders dar.

Insgesamt zeigt sich, dass die Aufgaben der Städte sehr umfangreich sind. Die Anforderungen an die Gesamtlösung entstammen aus unterschiedlichsten Bereichen. Alle Anforderungen müssen gesammelt und angegangen werden. Neben der Einführung der digitalen Signatur sollen Geschäftsvorfälle elektronisch durchgeführt und auch bezahlt werden. Allein diese drei Bereiche, ohne hier auf Datenschutz und Verfügbarkeit einzugehen, halten Probleme bereit, die bisher technisch nicht zufriedenstellend – auch nicht als Einzelprojekte – gelöst worden sind. Die Städte haben die schwierige Aufgabe, diese Einzelprojekte zusammenzuführen. Dabei sollen die eingesetzten Verfahren möglichst interoperabel sein. Der Aspekt der Interoperabilität und die Einforderung von Standards sind allerdings keine sicherheitstechnischen Bewertungsaspekte.

2.5 Ökonomische Voraussetzungen und Fragen [Autor: Busso Grabow (Difu)]

2.5.1 Individuelle Nutzenerwägungen – mikroökonomische Sicht

Online-Dienstleistungen der Verwaltung sollten durchgängig unter der Prämisse möglichst hoher Nutzenstiftung stehen. Dabei hat der erwartete Nutzen mehrere Bewertungsebenen:

- *Zeitersparnisse* (Wege-, Warte-, Prozesszeiten usw.),
- *Qualitäts-, Komfortsteigerung* (Individualisierung der Verfahren, Zeit-, Ortsunabhängigkeit, One-Stop-Service, Verstetigung des Arbeitsprozesses usw.),
- *Leistungsvolumen* (Umfang der Transaktionen und Geschäftsprozesse, Marktvolumen usw.),
- *Gewinn an Sicherheit* (Vermeidung von Fehlerfassung, Verminderung des Inkassorisikos, Wegfall von Verlustrisiken, Falschanzeigen usw.),
- *Kostensenkung* (Wegekosten, Transaktionskosten, economies of scale usw.),
- *Einnahmeerzielung* (Gebühren, Dienstleistungsentgelte, Lizenzeinnahmen usw.).

Alle sechs Bewertungsebenen haben auch ökonomische Dimensionen – direkt oder indirekt. Die Effekte treten sowohl bei den Anbietern von elektronischen Leistungen als auch bei den Nutzern auf, allerdings in unterschiedlichem Umfang (vgl. Übersicht).

Übersicht: Nutzen von elektronischen Verwaltungsdienstleistungen nach Gruppen – Plausibilitätsannahmen*

Nutzenkategorien	Verwaltung	Bürger	Unternehmen
Zeitersparnisse	✘	✘✘✘	✘✘
Qualitäts-, Komfortsteigerung	✘	✘✘✘	✘✘
Leistungsvolumen	✘✘	✘	✘
Gewinn an Sicherheit	✘		
Kostensenkung	✘	✘	✘
Einnahmeerzielung	teilweise ✘		✘

Die Zahl der Kreuze symbolisiert die Höhe des Nutzens.

*Quelle: Eigene Ausarbeitung.

Diffusionshemmnisse bei technikgestützten Dienstleistungsinnovationen bestehen häufig darin, dass Kosten und Erträge teilweise an unterschiedlichen Stellen anfallen. Beispielsweise können bei einfachen elektronischen Dienstleistungen auf der kommunalen Seite vor allem Kosten entstehen (beispielsweise beim Re-Engineering eines kompletten Verwaltungsverfahrens; vgl. Bremen) und auf Bürger- oder Unternehmensseite vor allem Nutzen.

Hier tritt dann die notwendige Unterscheidung der betriebswirtschaftlichen und volkswirtschaftlichen Betrachtungsweise hinzu. Auch betriebswirtschaftliche und volkswirtschaftliche Wirkungen können durchaus entgegenlaufend sein. So sind beispielsweise aufwendige Verfahren der Standardisierung aus betriebswirtschaftlicher Sicht bei den Entwicklern in der Regel kurz- und mittelfristig Kostenverursacher; die langfristigen volkswirtschaftlichen Aspekte sind jedoch positiv.

Das individuelle Nutzenkalkül geht in der Regel deutlich über den monetären Nutzen hinaus und bezieht auch immaterielle Aspekte, wie sie oben aufgeführt sind, ein. So wird in Nürnberg auch zwischen einer Kosten-/Erlös-Rechnung (die nur die direkten monetären Effekte umfasst) und einer Kosten-/Nutzen-Rechnung differenziert. Diese Unterscheidung ist generell notwendig, wenn man Online-Projekte der öffentlichen Verwaltung, gerade auch unter dem Einsatz der digitalen Signatur, zu bewerten versucht. Dabei reicht der Nutzenbegriff über den von Nürnberg verwendeten hinaus und berücksichtigt alle genannten Ebenen.

Für die Nutzung einer Online-Dienstleistung der Verwaltung muss der geldbewertete Nutzen so groß sein, dass er die Kosten übersteigt. Dies wird bei einem interaktiven Kontakt von Bürgern oder Unternehmen mit der Verwaltung über das Internet immer dann der Fall sein, wenn die Infrastruktur (z.B. der PC mit Internetanschluss zu Hause oder am Arbeitsplatz) vorhanden ist und – abgesehen von den Online-Nutzungsgebühren – keine weiteren Kosten anfallen.

Wird allerdings der Einsatz der digitalen Signatur erforderlich, können die Kosten und der Aufwand für die Anschaffung von Chip-Karten mit digitaler Signatur einschließlich der notwendigen Hardware sowie Infrastruktur für Bürger zunächst nicht unerheblich sein (zumindest bei der qualifizierten und akkreditierten Signatur), der Nutzen aus sporadischen Kontakten mit der Verwaltung zunächst nur gering. Daher ist für den Bürger ein Zusatznutzen aus Massenanwendungen (der nicht monetär sein muss) oder Einsparungen in anderen Angelegenheiten notwendig.

Bei privatwirtschaftlich agierenden Einrichtungen, wie beispielsweise den Mittlern elektronischer Dienstleistungen, muss mittelfristig nicht nur der Gesamtnutzen, sondern auch der direkte monetäre Nutzen die Kosten übersteigen; sie müssen mit ihren Dienstleistungen Erträge erwirtschaften.

Für Unternehmen spielen Schnelligkeit und Verfahrensverkürzung im Nutzenkalkül eine ähnliche große Rolle wie Leistungsvolumina und direkte Kosteneinsparungen.

Die Nutzenbewertung bei den öffentlichen Anbieter ist besonders schwierig. Bisher ist es so, dass sich die Online-Dienstleistungen von kommunalen Verwaltungen kaum monetär bemessen lassen. Hohen EDV-Investitionen stehen in der Regel zwar kostenrelevante Effizienzgewinne gegenüber, die aber nur schwer isoliert bewertet werden können. Für Verwaltungen können die Kosteneinsparungen erheblich sein; die Investitionen in Hard- und Software sowie die Kosten notwendiger Neuordnungen von Geschäftsprozessen werden sich allerdings frühestens mittel- bis langfristig amortisieren. Qualitative Nutzeneffekte (z.B. Zuverlässigkeit, Sicherheit, Verbesserung der Dienstleistungsqualität) sind zunächst höher zu bewerten als quantitative.

2.5.2 Volkswirtschaftlicher Nutzen – makroökonomische Sicht

Die individuelle und volkswirtschaftliche Nutzenbewertung mag – wie oben beschrieben – oft auseinander fallen. Generell kann man aber davon ausgehen, dass der volkswirtschaftliche Nutzen von Online-Dienstleistungen der Verwaltung unter Einbeziehung der digitalen Signatur im Hinblick auf Wertschöpfungseffekte und die Verbesserung der Standortqualität positiv ist. Schwieriger ist das Urteil bei den Wirkungen auf Arbeitsmarkt und Beschäftigung.

Die Entwicklung von Software, Hardware und Dienstleistungen für die Online-Verwaltung ist *wertschöpfungsintensiv*. Das Wachstum der IuK-Märkte betrug in Deutschland 1994 bis 1997 durchschnittlich sechs Prozent pro Jahr[49]. Nahezu sämtliche Großunternehmen sind heute in diesem Bereich aktiv und versuchen, sich Marktanteile zu erschließen und zu sichern. In Abhängigkeit von der Interoperabilität zwischen nationalen und europäischen oder internationalen Lösungen sind hiermit über die Binneneffekte hinaus auch Exportchancen verbunden. Dies muss auch deswegen von besonderem Interesse sein, weil das Wachstum der IuK-Märkte und der deutschen IuK-Wirtschaft in den 90er-Jahren hinter dem der Weltmärkte, auch dem der europäischen Märkte oder jenem der USA, hinterherhinkte[50]. Hier werden in den nächsten ein bis zwei Jahren entscheidende Weichenstellungen im Hinblick auf die internationalen Standards bei den Fragen Sicherheit und Geschäftsverkehr im Netz stattfinden.

Durch *Standardisierung* entsteht hoher volkswirtschaftlicher Nutzen. Dies gilt nicht nur für die technischen Grundlagen sicherer Online-Dienstleistungen im Netz, sondern auch für die Entwicklung der Anwendungen und der Software. Seit dem Zeitpunkt, als Internet, Intranet usw. erstmals zum Thema für die Kommunen wurden, gab es eine Vielzahl von Parallelentwicklungen bei Stadtinformationssystemen, Kiosksystemen, internem Informationsmanagement usw.[51] Zu Beginn war diese „chaotische“ Entwicklung möglicherweise kaum zu vermeiden; der volkswirtschaftliche Schaden durch Parallelentwicklungen und „Irrwege“ war erheblich. Inzwischen gibt es genügend gute Beispiele, die als Vorbild und zur Weiterentwicklung dienen können. *MEDIA*@Komm könnte erheblichen volkswirtschaftlichen Nutzen erzeugen, wenn es gelingt, in Bezug auf Online-Dienstleistungen der Verwaltung unter Nutzung der digitalen Signatur gewisse Standardisierungen und Nachahmereffekte zu erreichen.

Untersuchungen haben in den vergangenen Jahren immer wieder den besonderen Stellenwert des Umgangs der Verwaltung mit den Unternehmen, einfacher Behördenwege, von schnellen und transparenten Bearbeitungsvorgängen hervorgehoben[52]. On-

---

49 Vgl. statistische Beilage auf CD-ROM zu *Herbert Kubicek u.a. (Hrsg.),* Multimedia@Verwaltung, Heidelberg 1999 (Jahrbuch Telekommunikation und Gesellschaft, Bd. 7) des Fachverbandes Informationstechnik (FVIT) im Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA) und im Zentralverband Elektrotechnik und Elektronikindustrie e.V. (ZVEI), S. 23.

50 Vgl. ebenda.

51 Vgl. dazu z.B. *Steffi Bütow und Holger Floeting,* Elektronische Stadt- und Wirtschaftsinformationssysteme in deutschen Städten, Stuttgart 1999; *Busso Grabow und Holger Floeting,* Wege zur telematischen Stadt, in: Herbert Kubicek u.a. (Hrsg.), Multimedia@Verwaltung, Heidelberg 1999(Jahrbuch Telekommunikation und Gesellschaft Bd. 7); *Busso Grabow und Erwin Riedmann,* Kommunales Handlungsfeld IuK und neue Medien, Berlin 1998 (Deutsches Institut für Urbanistik, Reihe Aktuelle Informationen).

52 Vgl. zusammenfassend *Busso Grabow, Dietrich Henckel und Beate Hollbach-Grömig,* Weiche Standortfaktoren, Stuttgart 1995, S. 213 ff. (Schriften des Deutschen Instituts für Urbanistik, Bd. 89).

line-Dienstleistungen der Verwaltung unter Nutzung der digitalen Signatur machen genau dies möglich und erhöhen damit die *Standortqualität* durch Verbesserung der Dienstleistungen der Verwaltung. Der monetäre Nutzen beispielsweise von elektronisch beschleunigten Baugenehmigungsverfahren kann erheblich sein. Wie oben beschrieben, spielen für Unternehmen Schnelligkeit und Verfahrensverkürzung im Nutzenkalkül eine besonders große Rolle.

Die Studien der vergangenen Jahre zu den *Beschäftigungseffekten* der Informationsgesellschaft kommen zu deutlich widersprüchlichen Ergebnissen. Einem gewissen Arbeitsplatzwachstum in den neuen IuK-Branchen (selbst dies wird noch sehr unterschiedlich eingeschätzt und reicht von nur geringen Zuwächsen bis zu deutlichem Wachstum) stehen Rationalisierungseffekte durch den Einsatz der neuen Medien gegenüber[53]. Die berechneten Saldogrößen sind in einigen Untersuchungen sogar negativ. Die in den politischen Absichtserklärungen genannten Zahlen liegen im Normalfall weit über den in seriösen Schätzungen erwarteten Größen; die Saldoeffekte bleiben in der Regel ungenannt. Für Online-Dienstleistungen der Verwaltung unter Nutzung der digitalen Signatur gilt Entsprechendes: Durch die Erstellung von Produkten und Dienstleistungen in diesem Umfeld sind zwar positive Beschäftigungseffekte zu erwarten; diesen stehen aber auch Rationalisierungsmöglichkeiten gegenüber, etwa bei der elektronischen Führung von Grundbüchern, bei Auskunftsersuchen oder einer Reihe weiterer Projekte. Eine Abschätzung der Wirkungen ist äußerst schwierig und kann im Rahmen von *MEDIA*@Komm auch nur einzelfallbezogen versucht werden.

53 Vgl. z.B. die Ergebnisse und zitierten Studien in *Werner Willms*, Regionale Beschäftigungseffekte der Informationsgesellschaft (Monatsbericht des Bremer Ausschuss für Wirtschaftsforschung 12/1997); *Ute Bernhardt und Ingo Ruhmann*, Die Informationsgesellschaft ist keine Jobmaschine (Frankfurter Rundschau vom 5.1.1998); *Johann Welsch*, Der Telekommunikationssektor: „Beschäftigungslokomotive“ der Informationsgesellschaft (WSI-Mitteilungen 1/1998); „Studie: in einem Jahr 1,2 Mio. neue Internet-Jobs geschaffen“, in: I-Business-Nachrichten, www.hightext.de vom 17.6.99; *Martin Baethge u.a.*, Dienstleistungen als Chance: Entwicklungspfade für die Beschäftigung (Abschlußbericht eines Gutachten für das BMBF; zitiert in Frankfurter Rundschau vom 24.6.99); „Multimedia: Politiker haben den Mund zu voll genommen“ in: Computerwoche 26/99; „Mehr oder weniger? Zwei neue Internetstudien aus Deutschland geben Rätsel auf“ in: Berliner Zeitung vom 22.9.99; Informationstechnologien als Jobknüller (SPIEGEL-ONLINE – Netzdepesche vom 1.11.99; http://www.spiegel.de/netzwelt/politik/0,1518,49769,00.html) usw.

3. E-Commerce und E-Payment

3.1 E-Commerce-Diffusion [Autor: Holger Floeting (Difu)]

Für den Begriff *Electronic Commerce* gibt es bisher noch keine allgemein anerkannte Definition. Der Begriff umfasst unterschiedliche Geschäftsfelder und Tätigkeiten. Die Abgrenzungen zu anderen ähnlichen Begriffen wie Electronic Business, Teleshopping usw. sind nicht eindeutig. Im engeren Sinn versteht man unter Electronic Commerce „Verkauf und Bezahlung von Waren und Dienstleistungen über Telekommunikationsnetze, insbesondere das Internet." Weit gefasst lassen sich darunter alle Aktivitäten zusammenfassen, „die der betrieblichen Leistungserstellung dienen und über Telekommunikationsnetze abgewickelt werden".[54] Unterschieden werden dabei:

- die Unterstützung von Transaktionen zwischen Unternehmen durch IuK-Technologien (Business-to-Business),
- die Unterstützung von Transaktionen zwischen Unternehmen und privaten Haushalten durch IuK-Technologien (Business-to-Consumer) und
- die Unterstützung von Transaktionen zwischen Unternehmen und öffentlichen Verwaltungen durch IuK-Technologien (Business-to-Administration).

Im Folgenden werden die ersten beiden Bereiche behandelt. Online-Dienstleistungen der Verwaltung werden an anderer Stelle ausführlich dargestellt, sodass auf eine Darstellung der Business-to-Administration-Beziehungen hier verzichtet wird.

3.1.1 Business-to-Business

In Europa wurde 1999 mit Electronic Commerce im Business-to-Business-Bereich ein Umsatz von mehr als 33 Milliarden Euro erzielt. Weitere drei Milliarden Euro wurden im Business-to-Consumer-Bereich erwirtschaftet. Für das Jahr 2004 werden 1550 Milliarden Euro Umsatz prognostiziert. Allein für den deutschen Markt wird mit einem Umsatz von rund 406 Milliarden Euro gerechnet[55]. Mit der Entwicklung des E-Commerce werden also erhebliche Wachstumserwartungen verbunden. Gerade Unternehmen aus den Bereichen IuK-Technologien und allgemeine Dienstleistungen sehen die Entwicklung optimistisch. Betroffen von dieser Entwicklung werden aber viele Branchen sein. Dies gilt bereits in den nächsten zwei Jahren nach Einschätzung von Führungskräften gerade für die Bereiche Finanzwesen, Konsumgüter, Kommunikation und Unterhaltung

Electronic Commerce hat im Rahmen der strategischen Unternehmensplanung einen hohen Stellenwert[56]. Haben sich zuerst vor allem Großunternehmen mit der Nutzung

---

54 *Joachim Griese und Pascal Sieber (Hrsg.)*: Electronic Commerce, Aus Beispielen lernen, Zürich 1999, S. 112, zitiert nach: http://ec.unibe.ch/begriffe.asp (15. März 2000).

55 *Forrester Research* 1999, zitiert nach: http://www.electronic-commerce.org/fragen-antworten/frage-5.html (15. März 2000).

56 1998 wurde E-Commerce im Rahmen der KPMG-E-Commerce-Umfrage von Unternehmen mit 1. Priorität, 1999 mit 2. Priorität im Vergleich zu anderen strategischen Zielen bewertet. 1999 wurde kein Thema mit erster Priorität bewertet. Vgl. *KPMG*, Electronic Commerce, Status Quo und Perspektiven ´98, Berlin 1998, S. 11 und *KPMG*, Electronic Commerce, Status Quo und Perspektiven ´99, Berlin

des Internets und eigener Web-Präsenz beschäftigt, ist mittlerweile auch der deutsche Mittelstand stärker engagiert. In mittelständischen Dienstleistungsunternehmen haben 70 Prozent der Mitarbeiter Zugang zum Internet, in Handel und Industrie ist es immerhin noch mehr als die Hälfte[57]. Mehr als 60 Prozent der Mittelstandsunternehmen verfügen heute bereits über eine eigene Web-Seite.

Ähnlich wie bei den Kommunen ist aber auch im Unternehmensbereich die bisherige Web-Präsenz vor allem informationsorientiert. Mit Transaktionsangeboten hat sich bisher nur eine Minderheit der Mittelstandsunternehmen beschäftigt. Bislang setzen nur 14 Prozent von diesen E-Commerce-Lösungen ein, weitere 17 Prozent planen den Einsatz[58]. Vorreiter sind Handel und Dienstleistungsunternehmen. Größere Unternehmen nutzen E-Commerce-Lösungen in stärkerem Maß. Die Unternehmen reagieren damit nach eigenen Angaben vor allem auf Kundenanforderungen und wollen mit E-Commerce-Lösungen neue Wettbewerbschancen nutzen[59].

Positive Auswirkungen versprechen sich die Unternehmen vor allem für das Firmenimage, die Kommunikation mit Kunden und Zulieferern sowie die Kundenorientierung und -bindung[60]. Die Bedeutung der Kundenorientierung als Motivationsfaktor für die Nutzung von E-Commerce-Lösungen hat gegenüber den letzten Jahren zum Teil sogar zugenommen[61]. Die geringe Exportorientierung des deutschen Mittelstands spiegelt sich auch bei den erwarteten Auswirkungen des E-Commerce wider: Einstieg in das Auslandsgeschäft oder dessen Ausweitung spielen als angenommene positive Auswirkung nur eine untergeordnete Rolle[62].

Ähnlich wie im kommunalen Bereich fehlt auch bei den mittelständischen Unternehmen bisher weitgehend eine Verknüpfung zwischen der Web-Präsenz und DV-gestützten internen Geschäftsprozessen – und auch zukünftig wird eine derartige Verknüpfung nur von einem kleineren Teil der Unternehmen angestrebt: So wollen nur 15 Prozent der Mittelstandsunternehmen ihr www-Angebot an das Warenwirtschaftssystem anbinden. Deutlich stärker ist dieser Wunsch aber bei Handelsunternehmen ausgeprägt.

Im Vordergrund steht insgesamt weiterhin die Präsentation des Unternehmens und des Produktkatalogs. Auch hier zeigen sich Analogien zur Entwicklung im kommunalen Bereich: Die wichtigsten Elemente des Umgangs mit dem Internet sind die Darstellung der eigenen Organisation bzw. des eigenen Unternehmens, gefolgt von der Nutzung der Kommunikationsmöglichkeit via E-Mail und der Abrufmöglichkeit von anderen Fir-

---

1999, S. 9. Damit ist das Thema den Unternehmen genauso wichtig wie die Effizienzsteigerung und Kostensenkung oder das Customer Value Management. Befragt wurden Unternehmen und öffentliche Verwaltungen in Deutschland, Österreich und der Schweiz. 1998 lag der Schwerpunkt des Rücklaufs bei Unternehmen aus der IuK-Technologie, stark vertreten waren auch Beratungs- und Serviceunternehmen. 1999 war daneben auch der Anteil der Banken und Medienunternehmen überdurchschnittlich. Über 50 Prozent der Unternehmen waren in beiden Studien vertreten.

57 *Impulse/IBM*, Internet- und E-Business-Einsatz im bundesdeutschen Mittelstand, o.O. 1999, S. 51. Die Gesamtstichprobe umfasst 305 Fälle. Befragt wurden bundesdeutsche Unternehmen mit zehn bis unter 500 Mitarbeitern. 43 Prozent der Unternehmen gehören zur Industrie, 27 Prozent zum Dienstleistungsbereich, 21 Prozent zum Handel, neun Prozent zum Handwerk.

58 Ebenda, S. 14 ff.

59 Ebenda, S. 25 ff.

60 Ebenda, S. 28 ff.

61 *KPMG* 1999, S. 10.

62 *Impulse/IBM*, S. 28 ff.

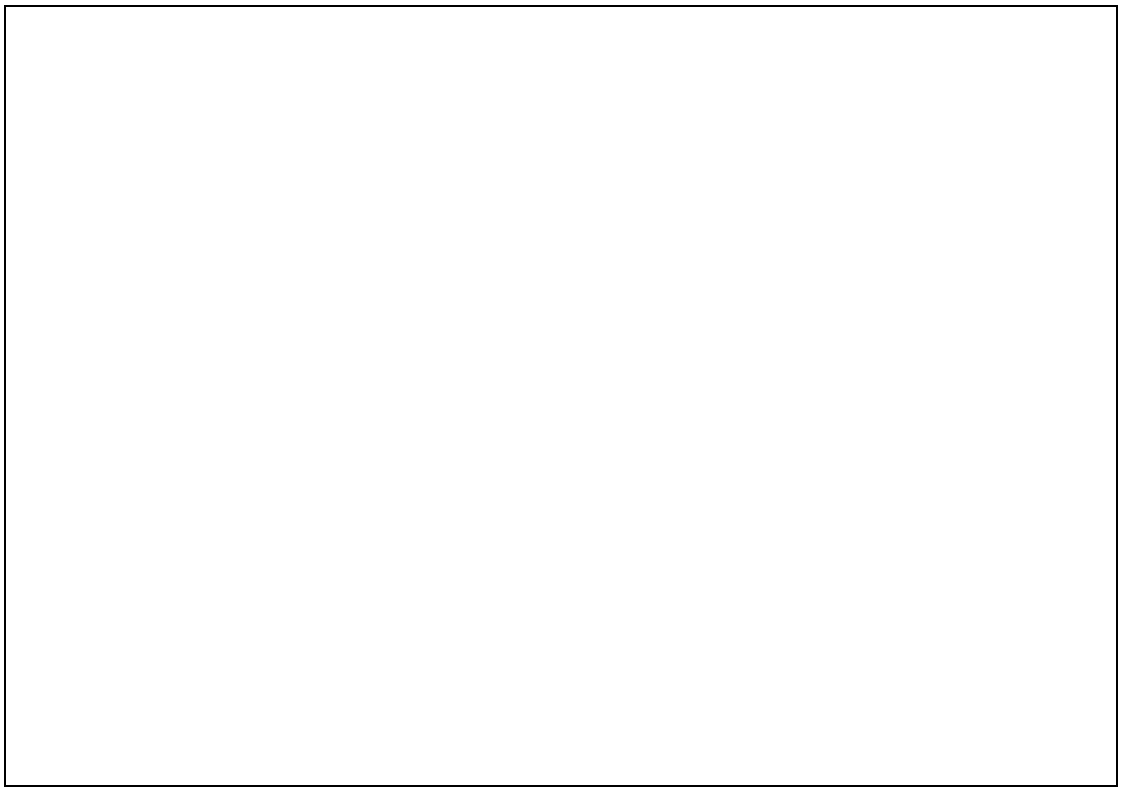
men-, Produkt- und Dienstleistungsinformationen. Der Ein- und Verkauf von Produkten und Dienstleistungen über das Internet ist demgegenüber nachrangig[63].

Die Angebote sollen aber insgesamt interaktiver werden. Drei Viertel der Mittelstandsunternehmen wollen beispielsweise ihren Produktkatalog mit Bestellmöglichkeiten versehen[64]. Der höchste Zuwachs liegt bei den interaktiven Komponenten Produkt- und Dienstleistungsverkauf, elektronische Archivierung, Videoconferencing und Internet-Telefonie[65]. Der Online-Vertrieb ist bisher aber für kaum einen Anbieter profitabel[66].

Wie im kommunalen Bereich verspricht man sich auch bei mehr als der Hälfte der mittelständischen Unternehmen zumindest punktuelle Produktivitätssteigerungen durch die Nutzung des Internets.

Auch beim Thema Kundentransparenz zeigen sich deutliche Analogien zwischen kommunalem Bereich und der mittelständischen Wirtschaft: Das Internet wird bisher wenig als Werkzeug zur Verbesserung der Kundentransparenz genutzt[67].

Abbildung:



63 *KPMG* 1999, S. 11 und *Impulse/IBM*, S. 37 ff.
64 *Impulse/IBM*, S. 34 ff.
65 Ebenda, S. 37 ff.
66 *Münchner Kreis* (Hrsg.), 2014, Die Zukunft von Information, Kommunikation und Medien, Expertenforum des Münchner Kreises, München 1999, S. 82.
67 *Impulse/IBM*, S. 42 ff., S. 58 ff.

E-Commerce wird sich bei den Mittelstandsunternehmen in Zukunft stärker vom Business-to-Consumer (B2C) zum Business-to-Business-Bereich (B2B) entwickeln. Schon heute entfallen von in Europa geschätzten Gesamtumsätzen im E-Commerce in Höhe von 36 Milliarden Euro nur drei Milliarden Euro auf den B2C-Bereich. Für 2004 rechnet man mit einer Verteilung von rund 1,5 Billionen Euro bei B2B und 232 Milliarden Euro bei B2C[68]. Auch wenn diese Schätzwerte sehr vage sind, zeigen sie einen Entwicklungstrend. Schon heute nutzen 13 Prozent der Unternehmen E-Commerce vorwiegend im B2B-Bereich, 24 Prozent ausschließlich[69]. Ähnliche Entwicklungen zeichnen sich auch im kommunalen Bereich ab, wo neben den Dienstleistungen für den Bürger immer stärker auch die Nutzung elektronischer Geschäftsprozesse im Umgang mit der Wirtschaft, mit Intermediären, die Bürgerdienstleistungen erbringen, und zur Kommunikation zwischen Gebietskörperschaften angeboten werden.

Sowohl der kommunale Bereich als auch die Wirtschaft müssen bei der Entwicklung ihrer Internet-Angebote bisher mit dem Problem umgehen, dass den Kunden die nötige technische Ausstattung fehlt bzw. die vorhandene technische Ausstattung unzureichend genutzt wird. Das Thema „fehlende Sicherheit" stellt nach wie vor sowohl in den Kommunen wie in der Wirtschaft einen Hinderungsgrund im Umgang mit E-Commerce dar. Das Problembewusstsein für dieses Thema ist in den Unternehmen nochmals gestiegen[70].

Ähnlich wie im kommunalen Bereich liegt ein wesentliches Problem in dem bisher fehlenden einheitlichen Transaktionsstandard. Mehr als ein Fünftel der kleinen Unternehmen (bis 49 Mitarbeiter) sehen darin das Problem Nummer 1 im Umgang mit E-Commerce.

Online-Bezahlung, -Bestellung, -Belieferungen sind „heute noch vergleichsweise selten implementiert"[71]. Erst 15 Prozent der befragten Unternehmen nutzen das Internet für integrierte Zahlungsvorgänge, obwohl 45 Prozent Bankgeschäfte über Internet oder Online-Dienste tätigen[72]. Auffällig ist auch die große Bedeutung, die das Thema elektronische Identifikation/Authentifizierung als Problem im Umgang mit dem E-Commerce für den Handel hat – ein Thema, das auch im Vordergrund der Entwicklungen im kommunalen Bereich steht[73].

Ähnliches gilt für das beklagte Wissensdefizit bei Entscheidern. Sowohl in den Unternehmen wie im kommunalen Bereich bestehen hier erhebliche Lücken. Diese Wissensdefizite scheinen die Entwicklung von E-Commerce-Lösungen auch in immer größerem Umfang zu behindern. Der Anteil der Unternehmen, die dies für eine Barriere halten, ist jedenfalls gestiegen[74].

---

68 *Forrester Research* 1999, zitiert nach: www.electronic-commerce.org/marktbarometer/daten/umsatz (4. Februar 1999).
69 *Impulse/IBM*, S. 78 ff.
70 45 Prozent der befragten Unternehmen in der KPMG-Studie 1999 sehen im Thema Sicherheit einen Hinderungsgrund gegenüber 33 Prozent 1998. Vgl. *KPMG* 1998, S. 12 und *KPMG* 1999, S. 10.
71 *KPMG* 1999, S. 11.
72 Ebenda.
73 *Impulse/IBM*, S. 98 ff.
74 Vgl. *KPMG* 1998, S. 12 und *KPMG* 1999, S. 11.

3.1.2 Business-to-Consumer

Zu den interaktiven Online-Konsumenten gehören nach unterschiedlichen Untersuchungen zwischen 3,7 Prozent[75] und sechs Prozent[76] der Bevölkerung in Deutschland. 35 Prozent der Online-Nutzer in Deutschland haben schon einmal ein Onlineshopping-Angebot genutzt, 31 Prozent schon einmal eine Buchbestellung online aufgegeben[77]. Zu den am meisten gekauften Produkten gehören Bücher, CDs und Software. Besonders hohe Wachstumsraten verzeichnen Produkte wie Kleidung, Textilien und Sportartikel[78]. Insgesamt ist der Anteil der Online-Käufer aber noch gering. Drei Prozent der Haushalte haben zumindest gelegentlich Bücher, CDs oder Videos im Internet eingekauft, zwei Prozent der Haushalte Computer Hard- und Software oder Kleidung, deutlich unter ein Prozent Lebensmittel und sonstige Haushaltswaren[79].

Der Gesamtumsatz deutscher Onlineshops wird in unterschiedlichen Untersuchungen für 1998 zwischen 420 Millionen DM und 700 Millionen DM angegeben. Der größte Teil des Umsatzes (80 bis 85 Prozent) gehört aber zum B2B-Bereich[80].

Ein Drittel der Internet-Nutzer hat bisher Online-*Dienstleistungen* in Anspruch genommen. Online-Banking steht dabei an erster Stelle. Eine große Entwicklungsdynamik ist bei Buchungen von Flug- und Bahntickets sowie Reisen und Hotels zu verzeichnen. Die größten Wachstumsraten weisen Auktionen, Telekommunikationsdienstleistungen und Versandhauseinkäufe auf.

Der typische deutsche Online-Konsument kommt eher aus städtischen Regionen, verfügt über ein überdurchschnittliches Einkommen und ist formal besser gebildet als der Bundesdurchschnitt[81].

Die Entwicklung des E-Commerce im B2C-Bereich wird vor allem beeinflusst durch[82]:

- die Netzinfrastruktur-Entwicklung,
- die Geräte-Entwicklung,
- die Diffusion von Online-Zugängen,
- die Entwicklung der Telekommunikationstarife,
- Datenschutz und -sicherheit,
- Marktentwicklungen, z.B. wie traditionelle und neue Anbieter sich positionieren,
- die Käuferakzeptanz für Onlineshopping.

---

75 *Frankfurter Allgemeine Zeitung* vom 1. Juni 1999
76 Münchner Kreis, S. 82.
77 *ARD/ZDF-Online-Studie 1999*, in: Media Perspektiven 8/99, S. 401-414, hier: S. 404.
78 *GFK Online-Monitor*, Pressemitteilung vom 18. August 1999, vgl. *auch FirstSurf Internetshoppingstudie 1998/1999*, zitiert nach idw vom 23. September 1999.
79 *Münchner Kreis*, S. 82.
80 Käufe bei ausländischen Anbietern und Direktkäufe bei Herstellern sind nicht eingeschossen, sodass der gesamte Umsatz für E-Shopping höher liegt. Ebenfalls nicht enthalten ist der B2B-Bereich, der den Hauptanteil von E-Commerce ausmacht. Vgl. *Münchner Kreis*, S. 82.
81 *Frankfurter Allgemeine Zeitung* vom 1. Juni 1999
82 *Münchner Kreis*, S. 83.

3.2 Elektronische Marktplätze [Autor: Holger Floeting (Difu)]

Elektronische Marktplätze können als wirtschaftsnahe Infrastruktur ähnlich den Energie-, Verkehrs- oder Telekommunikationsnetzen angesehen werden. Sie schaffen „enträumlichte" Märkte, auf die weltweit Zugriff genommen werden kann. In den USA gibt es mittlerweile zahlreiche virtuelle Shopping- und Dienstleistungszentren dieser Art, in denen in erster Linie kleine und mittlere Unternehmen Waren und Dienstleistungen anbieten. Auch in Deutschland haben sich in kurzer Zeit Plattformen entwickelt, die z.B. elektronische „Auktionen" anbieten. Die Ausrichtung auf die Belange einer bestimmten Region fehlt bei diesen Beispielen aber weitgehend.

Bisher gibt es nur vereinzelt Beispiele für eine regionale Ausrichtung. Beispiele für derartige Projekte sind[83]:

- der virtuelle Marktplatz der Kreissparkasse Alzey[84],
- Der Norden – Marktplatz Bremerhaven[85],
- Marktplatz CW – Der virtuelle Treffpunkt für den Kreis Calw und die Region Nordschwarzwald[86],
- der virtuelle Marktplatz der Kreissparkasse Freiberg[87],
- Marktplatz für die Region Göppingen[88],
- KISS MARKTPLATZ[89],
- Marktplatz Krefeld[90],
- der Marktplatz der Sparkasse Neuwied[91],
- Virtueller Marktplatz Oberharz[92],
- Marktplatz Osnabrücker Land[93],
- Marktplatz der Kreissparkasse Osterholz[94],
- Harzweb – der Marktplatz des Landkreises Osterode[95],
- Marktplatz Osterode[96],
- Virtuelle Schmuckmesse Pforzheim[97],
- Virtueller Marktplatz der Stadtsparkasse Witten[98].

Weitere Vorhaben sind gerade in der Planung oder Umsetzung, wie etwa die regionalen Marktplätze im Bayern-Net, die gemeinde4u-Initiative des Niedersächsischen Städte- und Gemeindebundes oder die von dem Deutschen Sparkassen- und Giroverband initiierten und konzipierten regionalen Marktplätze der Sparkassen. Schließlich

83 Beispiele für Projekte unter Beteiligung der S-Finanzgruppe.
84 http://www.marktplatz-rheinhessen.de/ (9. Februar 2000).
85 http://www.der-norden.de/, (9. Februar 2000).
86 http://www.marktplatz-cw.de/, (9. Februar 2000).
87 http://www.freiberg-regional.de/, (9. Februar 2000).
88 http://www.marktplatz-gp.de/, (9. Februar 2000).
89 http://www.kiss-net.de/, (9. Februar 2000).
90 http://www.marktplatz-krefeld.de/, (9. Februar 2000).
91 http://www.marktplatz-neuwied.de/, (9. Februar 2000).
92 http://www.marktplatz-oberharz.de/, (9. Februar 2000).
93 http://www.marktplatz-osnabrueck.de/, (9. Februar 2000).
94 http://www.marktplatz-osterholz.de/, (9. Februar 2000).
95 http://www.harz-web.de/, (9. Februar 2000).
96 http://www.marktplatz-osterode.de/, (9. Februar 2000).
97 http://www.schmuckmesse.de/, (9. Februar 2000).
98 http://www.shopline-witten.de/, (9. Februar 2000).

versuchen auch verschiedene Städte unabhängig von solchen Gemeinschaftsinitiativen, virtuelle Marktplätze im Rahmen ihrer Stadtinformationssysteme zu installieren.

Die Konzepte dieser regionalisierten Ansätze gleichen einem virtuellen Warenhaus, in dem Produkte und Dienstleistungen unterschiedlichster Art angeboten werden. Die Grenzen zwischen Groß- und Einzelhandel verwischen dabei, d.h., die Angebote wenden sich sowohl an Privat- als auch Geschäftskunden[99]. Untersuchungen über die Verbreitung von elektronischen Marktplätzen mit regionalem Bezug liegen bisher nicht vor.

99 Als erster regional orientierter Marktplatz in Deutschland entstand bereits 1995 die Electronic Mall Bodensee (EMB), als virtuelles Forum für Bürger und Wirtschaft in der länderübergreifenden Region Bodensee. Zur Entwicklung der EMB vgl. auch *Steffi Bütow und Holger Floeting*, Elektronische Stadt- und Wirtschaftsinformationssysteme in den deutschen Städten, Stuttgart 1999, S. 151 ff.

3.3 Electronic Payment [Autorin: Christine Siegfried (Difu)]

Mit der steigenden Bedeutung von E-Commerce und den zunehmenden Möglichkeiten des Online-Shopping wächst auch die Bedeutung des elektronischen Bezahlens oder – „neudeutsch“ – „Electronic Payment”. Die einfachste Möglichkeit, einen Online-Kauf über das Internet zu tätigen, besteht in der Bestellung eines Artikels und dem Bezahlen mit Kreditkarte. Zugleich ist dies auch die unsicherste Variante, denn nichts ist unsicherer als die unverschlüsselte Übertragung von Kreditkartennummern über das Internet, weil jeder diese Nummer „abfangen” und für seine eigenen Zwecke auf Kosten des eigentlichen Kreditkarteninhabers verwenden kann.

Die Zahl der Online-Shops und Web-Anbieter wächst zwar stetig, aber 65 Prozent der deutschen Web-Shops bevorzugten 1999 noch immer die traditionellen Papierrechnungen oder liefern per Nachnahme (39 Prozent)[100]. Dies liegt vor allem an der fehlenden Interoperabilität, d.h., in der Regel ist eine komplizierte Integration von elektronischen Zahlungssystemen in die vorhandene Online-Shop-Software bei den Händlern notwendig. Problematisch ist dabei auch die noch geringe Verbreitung von benötigten Zusatzgeräten wie Kartenlesern oder der komplizierte Umgang mit zuvor zu installierender Software auf dem PC des Kunden. Begriffe wie SET, SSL, Cybercash, Cybercoin, EC-Cash, POS, POZ und andere Namen aus dem Bereich des Electronic Payment werden immer wieder genannt , ohne dass sie über den Kreis der damit beschäftigten Fachleute hinaus bei Händlern und Kunden einen erkennbaren Durchbruch, was die Nutzung betrifft, geschafft hätten. Im Folgenden sollen die wichtigsten Begriffe kurz erläutert und der Stand der Umsetzung von Electronic Payment geschildert werden.

3.3.1 Elektronisches Bezahlen mit der EC-Karte: POS/POZ, ELV

Einkaufen und Bezahlen mit den von den Kreditinstituten ausgegebenen EC-Karten (so genannten Debitkarten in Abgrenzung zur Kreditkarte) ist weit verbreitet und fällt unter die Rubrik elektronisches Bezahlen. Beim so genannten EC-Cash wird entweder beim Bezahlen eine Autorisierung des Kunden durch die Eingabe der PIN-Nummer vorgenommen (POS-Verfahren), oder es wird ein Lastschriftbeleg erstellt, der vom Kunden unterschrieben und vom Händler bei der Kundenbank eingereicht wird (elektronisches Lastschriftverfahren ELV). Als Variante zum POS gibt es noch das POZ-Verfahren, bei dem keine Autorisierung der Karte am Terminal erfolgt, sondern lediglich anhand vorhandener Sperrlisten eine Überprüfung vorgenommen wird. Für die Händler haben die verschiedenen Verfahren unterschiedliche Auswirkungen in Bezug auf die anfallenden Gebühren bzw. Telefonkosten und die Zahlungsgarantie.

3.3.2 Einkaufen im Internet mit Kreditkarte: SET und SSL

Eine sichere Möglichkeit des Bezahlens per Kreditkarte im Internet besteht in der Nutzung von SET (Secure Electronic Transaction). Dabei handelt es sich um ein Protokoll

100 Angaben des Hauptverbandes des Deutschen Einzelhandels, zitiert nach *Computerwoche* 8/99, S. 31.

für sicheren Zahlungsverkehr, das von großen Kreditkartenorganisationen wie Visa, Mastercard usw. in Kooperation mit großen Computerfirmen wie Microsoft, IBM und anderen als offener Standard entwickelt worden ist und im Jahr 1997 zum ersten Mal veröffentlicht wurde. SET kombiniert verschiedene kryptographische Verfahren sowohl für die Verschlüsselung der übertragenen Daten als auch für die Authentifizierung der am Zahlungsverkehr beteiligten Partner. Zentraler Ansatzpunkt sind Zertifikate, mit denen sich sowohl der Kunde als Karteninhaber als auch der Händler als berechtigter Abwickler ausweisen kann. Allgemein wird schon seit längerem erwartet, dass sich SET als Standard durchsetzen wird, weil es unabhängig von der eingesetzten Software auf Händler- und Kundenseite und nicht auf bestimmte Zahlungsverfahren festgelegt ist. Bis heute ist dies allerdings nicht geschehen. Als Grund hierfür gilt die hohe Komplexität des Verfahrens, bei dem Kunden, Händler und Finanzdienstleister unterschiedliche Programme installieren und alle mit Zertifikaten ausgestattet sein müssen. Deshalb erscheint SET auch bei Beträgen unterhalb der 10-DM-Grenze ungeeignet[101].

Ein anderes Protokoll zur sicheren Verschlüsselung von Daten, die im Internet-Zahlungsverkehr anfallen, ist SSL (Secure Socket Layer). SSL wurde 1994 von Netscape entwickelt und wird mittlerweile häufig eingesetzt. Zu erkennen ist es an den https-Adressen, die anzeigen, dass eine verschlüsselte Übermittlung (vor allem von Kreditkarteninformationen) stattfindet. Beim Beginn einer SSL-Sitzung schickt der Browser seinen öffentlichen Schlüssel an einen Server, der dann einen geheimen Schlüssel versenden kann. Auf dieser Grundlage findet dann die weitere Kommunikation statt. Als gravierender Nachteil von SSL wird gesehen, dass keine Authentifizierung des Absenders stattfindet. Dennoch ist SSL mittlerweile weit verbreitet.

3.3.3 Elektronisches („virtuelles") Geld: ECash, CyberCash, Geldkarte

3.3.3.1 Ecash

Im Ecash-System der früheren Firma Digicash, das im Pilotversuch von der Deutschen Bank getestet wurde, werden im Prinzip elektronische Münzen hergestellt und wie normale Münzen zum Bezahlen eingesetzt. Dieses System konnte sich bisher nicht durchsetzen – nicht nur aufgrund des Konkurses der Firma Digicash, sondern vor allem wegen der hohen Kosten und der befürchteten Auswirkungen auf den nationalen und internationalen Geldmarkt bei der Generierung von „Netzgeld".

3.3.3.2 CyberCash

Im Gegensatz zu Ecash basiert CyberCoin der Firma CyberCash nicht auf Münzen, sondern auf Kontobuchungen, sodass kein echtes Netzgeld entsteht. Ähnlich wie bei der Debitkarte wird auf ein Konto zugegriffen, allerdings nicht auf ein reales Girokonto, sondern auf ein virtuelles oder so genanntes Schattenkonto, das in diesem System Cash-Container genannt wird. Ein Pilotvorhaben wurde in Deutschland unter Beteiligung der Dresdner Bank und der Commerzbank durchgeführt. Anfang des Jahres 2000

101 *K. Böhle und U. Riehm*, Blütenträume – Über Zahlungssysteminnovationen und Internet-Handel in Deutschland, Karlsruhe 1998, S. 51 ff.

sind insgesamt elf Banken an dem Vorhaben beteiligt. Ein Blick auf die WWW-Seite cybercash.de zeigt im Januar 2000 eine Liste mit rund 40 „Partnern", die das System unterstützen, sowie etwa 50 Händlern, bei denen man mit CyberCash einkaufen kann[102]. Die Tatsache, dass mittlerweile über die Initiatoren Dresdner Bank und Commerzbank weitere Banken sich an Ecash beteiligen, scheint die ursprüngliche Skepsis hinsichtlich der Frage, ob die Banken überhaupt Interesse an einer solchen Entwicklung haben, zu widerlegen[103]. Erst im November 1999 hat die Baden-Württembergische Landesbank ihren Kunden den CyberCash-Service offeriert und ihnen angeboten, ab sofort die entsprechende Software von den Internetseiten der Bank herunterzuladen[104]. Die andere Frage, ob CyberCash nicht die gleiche Funktionalität biete wie die Geldkarte, die eine „fortschrittliche" Chipkartenlösung darstellt und daher dem CyberCash überlegen ist, lässt sich erst dann beantworten, wenn umfangreichere Erfahrungen mit dem Chipkarteneinsatz ausgewertet werden können.

3.3.3.3 Geldkarte

Die elektronische Geldbörse oder Geldkarte ersetzt das Bargeld. Bei diesem Prinzip wird das Konto des Inhabers im voraus mit dem Geld belastet, das er sich an entsprechenden Ladestationen (Banken, Sparkassen) auf die Karte lädt oder bar einzahlt. Die auf dem Chip gespeicherte Summe kann dann zum Einkaufen verwendet werden (prepaid) – und zwar sowohl offline als auch online. Die EC- wie auch die Kunden-Karten der Banken und Sparkassen enthalten einen spezifischen Chip, auf dem die Geldkartenfunktion hinterlegt werden kann. Dieser Chip ermöglicht auch so genannte Zusatzanwendungen wie elektronische Fahrscheine, Parkscheine oder auch Bonussysteme des Handels[105].

Mitte des Jahres 1999 haben sich die im Zentralen Kreditausschuss (ZKA) vertretenen Banken und Sparkassen auf die elektronische Geldkarte als Online-Internet-Zahlungsverfahren geeinigt. Wichtiger Anreiz dafür waren neben der Sicherheit durch die Begrenzung der Geldmenge (DM 400,–) eben auch die möglichen Zusatzfunktionen auf den Chipkarten. Banken und Handel sind optimistisch, dass die Zahlungsfunktion auf dem Chip den Online-Handel schwunghaft beleben wird. Die weite Verbreitung der Bankkarten gilt quasi als Garant dafür, dass der Nutzerkreis zumindest potenziell ungeheuer groß ist. Wenn dann auf dem Geldkartenchip neben der Bezahlfunktion weitere Zusatzfunktionen wie elektronischer Fahrschein oder gar der Schlüssel für eine elektronische Signatur abgelegt werden können, versprechen sich Banken und Handel eine größere Akzeptanz. Sobald sich die Ausstattung der Kunden mit den notwendigen Lesegeräten deutlich verbessert, kann man davon ausgehen, dass die Geldkarte zum Einkaufen im Internet tatsächlich eine attraktive Alternative zu den bisher geschilderten Möglichkeiten darstellt. Wann und wie dieses Ziel erreicht werden kann, ist zur Zeit offen. Die bisher im Einsatz befindliche Geldkarte, mit der man offline bei entsprechend gekennzeichneten Akzeptanzstellen einkaufen kann, gilt dagegen im Handel eher als

102 Vgl. www.cybercash.de vom 06.01.00.
103 Vgl. *Böhle/Riehm*, S. 65.
104 Vgl. *I-Business-Nachrichten* vom 16.11.99: Landesbank Baden-Württemberg startet mit Cybercash, www.hightext.de.
105 Derzeit in Eichstätt und Kulmbach im Einsatz.

Flop. Ihr Anteil als Zahlungsmittel am Einzelhandels-Umsatz lag 1998 verschwindend gering bei weniger als 0,1 Prozent, während das elektronische Lastschriftverfahren 10,0 Prozent und die Kreditkartenzahlungen immerhin noch einen Anteil von 3,5 Prozent erreichten[106].

3.3.3.4 Internetbanking: HBCI und OTP

Der HBCI-Standard (Homebanking Computer Interface) wurde zur sicheren Durchführung von Transaktionen zwischen Kunde und Bank entwickelt. Es handelt sich dabei um einen Kommunikationsstandard zur Tätigung von Transaktionen zwischen intelligenten Kundensystemen und dem Bankensystem. Ursprünglich entwickelt wurde er für Homebanking, für das es bis dahin keinen Standard gab. Der ZKA hat HBCI Ende 1996 als Standard verabschiedet, derzeit liegt die Version 3.0 vor. HBCI definiert verschiedene Geschäftsvorfälle, wie z.B. Überweisungen, Saldoabfragen, Wertpapiergeschäfte usw.[107]

HBCI ist zwar kein elektronisches System, das einen Bezahlvorgang im Internet ermöglicht, dennoch soll an dieser Stelle auf die Bedeutung von HBCI und OTP (Open Trading Protocol) als „Grundmuster" für einen noch in der Entwicklung befindlichen Standard eingegangen werden, der sowohl die zu beachtenden Sicherheits- und Verschlüsselungs- als auch die Authentifizierungsaspekte im Internet berücksichtigt. Es gibt erkennbare Bestrebungen der Kreditwirtschaft und des Handels sowie von Softwarefirmen zur Förderung und Vereinfachung von E-Commerce durch die Entwicklung von gemeinsamen Standards (z.B. auf der Grundlage von HBCI), die in der Lage sind, die Transaktionen zwischen Händlern, Kunden und den Banken komplett durchzuführen. Im Rahmen von *MEDIA*@Komm spielt HBCI beim Bremer Vorhaben eine große Rolle, weil dort – aufbauend auf HBCI – ein Standard OSCI (Online Services Computer Interface) entwickelt werden soll, der die Durchführung aller anfallenden Geschäftsprozesse innerhalb der Verwaltung bei der Verwirklichung von deren Online-Dienstleistungen bewältigen kann.

106 Elektronischer Zahlungsverkehr: „Schmutziges POS", in: Handelsjournal 9/99, S. 9.
107 *Kurt Hauber*, HBCI-Kompendium, abzurufen unter www.sixsigma.de.

3.4 Rechtliche Aspekte von Electronic Commerce und Electronic Payment [Autoren: Martin Eifert, Lutz Schreiber, Claudia Stapel-Schulz (HBI)]

Die rechtlichen Fragen des E-Commerce und E-Payment bilden einen eigenen Fragenkreis mit allenfalls loser Anbindung an die *MEDIA*@Komm-Projekte, der nicht von der Begleitforschung zu *MEDIA*@Komm abgedeckt wird. Nachfolgend wird dementsprechend nur kurz der sich entwickelnde Rechtsrahmen für diese Bereiche zur Abrundung des Status quo-Berichts skizziert.

3.4.1 Die EU-Richtlinie zum Electronic Commerce

Mit einem Vorschlag zur Regelung rechtlicher Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt veröffentlichte die Europäische Kommission im November 1998 ihren Entwurf für eine Electronic-Commerce-Richtlinie[108]. Ziel des Entwurfs ist das einwandfreie Funktionieren des Binnenmarktes, insbesondere des freien Verkehrs von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten (Art. 1 Ril.). Am 4. Mai 2000 wurde die Richtlinie vom Europäischen Parlament angenommen; sie wird nun nach Veröffentlichung im amtlichen Anzeiger binnen 18 Monaten von den Mitgliedstaaten in nationales Recht umzusetzen sein[109].

Die Richtlinie ist grundsätzlich auf Dienste der Informationsgesellschaft[110] anwendbar (Art. 2 Ril.), die interaktive, im Fernabsatz und auf elektronischem Wege erbrachte Dienstleistungen sind. Als Beispiel hierfür kann Video-On-Demand genannt werden. Die Richtlinie beschränkt sich auf wirtschaftlich orientierte Diensteanbieter und fällt damit nicht in den Regelungsbereich der Verwaltungsdienstleistungen[111].

Entscheidende Regelung des Vorschlags ist die Festlegung des Herkunftslandprinzips (Art. 3 Ril.)[112], also die Verpflichtung, dass ein Dienst der Informationsgesellschaft, der in einem Mitgliedstaat rechtmäßig erbracht wird, im Zugang zum Binnenmarkt nicht behindert werden darf. Die Aufsicht über den Dienst obliegt dabei dem Mitgliedstaat, in dem der Dienst niedergelassen ist. Abweichungen hiervon sind jedoch ausdrücklich zugelassen (Art. 22 und Anhang I und II der Ril.).

Der Richtlinienvorschlag ist im Übrigen in weitere Kapitel gegliedert, wobei deren zweites das eigentliche „Herzstück" bildet. Es beinhaltet vier Teile, welche sich mit der Niederlassung von Anbietern und Informationspflichten (Art. 4 und 5 Ril.), der kommerziellen Kommunikation (Art. 6 bis 8 Ril.), elektronischen Verträgen (Art. 9 bis 11 Ril.) und der Verantwortlichkeit von Diensteanbietern (Art. 12 bis 15 Ril.) beschäftigen.

---

108 Die nun aktuelle Fassung (Stand: Gemeinsamer Standpunkt des Rates und der Kommission) ist abzurufen unter: http://europa.eu.int/comm/dg15/de/media/ecommerce/index.htm.

109 Vgl. Mitteilung der Kommission zur Annahme der Richtlinie vom 4. Mai 2000; abzurufen unter: http://europa.eu.int/comm/internal_market/en/media/eleccomm/2k-442.htm (englische Fassung).

110 Begriff im Sinne von Art. 1 Nr. 2 der Ril 98/34/EG (ABl. L 204 vom 21.7.1998, S. 37) in der Fassung der Richtlinie 98/48/EG (ABl. L 217 vom 5.8.1998, S. 18) – „Transparenzrichtlinie".

111 Vgl. nur *Spindler*, Der neue Vorschlag einer E-Commerce-Richtlinie, ZUM 1999, S. 775 f.; *Maennel*, Elektronischer Geschäftsverkehr ohne Grenzen – der Richtlinienvorschlag der Europäischen Kommission, MMR 1999, S. 187 f.

112 Vgl. zur Diskussion hierüber statt vieler: *Hoeren*, Vorschlag für eine EU-Richtlinie über E-Commerce, MMR 1999, S. 192, 194 ff.; *Spindler*, S. 780 ff.; jeweils mit weiteren Nachweisen.

Im Übrigen befasst sich der Richtlinien-Vorschlag mit der Umsetzung der Richtlinie, der außergerichtlichen Streitbeilegung auf elektronischem Wege und Ausnahmebestimmungen hinsichtlich ihrer Anwendung. Die Verabschiedung der Richtlinie ist für das Jahr 2000 vorgesehen.

3.4.2 Fernabsatzrichtlinie

Die Richtlinie 97/7/EG des Europäischen Parlaments und des Rates vom 20. Mai 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz[113] wurde zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über Vertragsabschlüsse im Fernabsatz zwischen Verbrauchern und Lieferern konzipiert, um Verbraucherschutz bei den modernen Distanzvertriebsformen wie Teleshopping, aber auch Versandhandel und Katalogverkauf zu vereinheitlichen. Damit setzt die EU ihre Verbraucherschutzpolitik auf der Linie der Haustürgeschäftswiderrufs-, der Verbraucherkredit- und der Time-Sharing-Richtlinie fort. Die Fernabsatzrichtlinie muss nach ihrem Artikel 15 bis zum Ablauf des 4. Juni 2000 in deutsches Recht umgesetzt werden. Ein deutsches Fernabsatzgesetz ist mittlerweile durch den Bundestag am 14.4.2000 verabschiedet worden[114]. Das Gesetz sollte am 1.6.2000 in Kraft treten. Der Bundesrat hat hierzu den Vermittlungsausschuss angerufen[115], sodass der vorgesehene Zeitplan nicht eingehalten werden wird.

Die wichtigsten Schutzinstrumente der Richtlinie zur Vermeidung der Risiken eines vereinfachten und grenzüberschreitenden Distanzvertriebs sind eine umfassende Informationspflicht des Anbieters (Art. 4 und 5 Ril.) und ein Widerrufsrecht des Verbrauchers binnen sieben Tagen (Art. 6 Ril.)[116]. Hervorzuheben ist, dass ein Verbraucher auf diese Schutzinstrumente nicht verzichten kann (Art. 12 Ril.).

Des Weiteren beinhaltet die Richtlinie Vorschriften zur Erfüllung des Vertrages (Art. 7 Ril.), zum Schutz vor betrügerischer Verwendung von Kreditkarten und der Zusendung unbestellter Waren sowie der Erbringung von Dienstleistungen (Art. 8 und 9 Ril.), zur Festschreibung des Opt-in bei kommerzieller Kommunikation mit Ausnahme von Telefax und Voice-Mail (Art. 10 Ril.); sie legt darüber hinaus Grundsätze für die Beteiligung öffentlicher Einrichtungen und Verbraucherverbände zur Einhaltung der Bestimmungen durch eigene Rechtsbehelfe fest (Art. 11 Ril.).

3.4.3 Elektronischer Zahlungsverkehr

Die regulatorischen Anstrengungen im Bereich des elektronischen Zahlungsverkehrs bleiben hinter den beschriebenen Ansätzen für den E-Commerce zurück. Zwar gab es Empfehlungen und Mitteilungen der EU-Kommission wie der Bundesregierung, die

113 ABl. L 144 vom 4.6.1998, S. 212.

114 Vgl. den Entwurf eines Gesetzes über Fernabsatzverträge und andere Fragen des Verbraucherrechts sowie zur Umstellung von Vorschriften auf Euro vom 9.2.2000, *BT-DrS.* 14/2658.

115 Vgl. Pressemitteilung des Bundesrates vom 19.5.2000; abzurufen unter http://www.bundesrat.de/-pr/pr69_00.html (Stand: 22.5.2000).

116 Der deutsche Entwurf sieht hierzu eine Widerrufsfrist von vierzehn Tagen vor, § 3 Abs. 1 FernAG-E, § 361a Abs. 1 BGB-E.

auch zu einer Förderung des elektronischen Zahlungsverkehrs beitragen sollten, eine rechtliche Regulierung ist jedoch bislang nicht erfolgt. Auf nationaler Ebene wurden allerdings mit der am 1. Januar 1998 in Kraft getretenen sechsten Novelle des Kreditwesengesetzes[117] sowohl vorausbezahlte Karten als auch Netzgeldgeschäfte der Aufsicht des Bundesamtes für das Kreditwesen unterstellt[118].

Im Gegensatz etwa zu den Schriftformerfordernissen hinsichtlich des Einsatzes der elektronischen Signatur bestehen im Bereich des elektronischen Zahlungsverkehrs allerdings auch keine bedeutsamen rechtlichen Hemmnisse[119].

117 BGBl. 1997, I, Nr. 71/2518 v. 28.10.1997.

118 Vgl. näher *Holznagel/Tabbara*, Politische Initiativen zum elektronischen Zahlungsverkehr, in: Holznagel/Hoeren, Rechtliche Rahmenbedingungen des elektronischen Zahlungsverkehrs, 1999, S. 19 ff.

119 Vgl. näher *Holznagel/Tabbara*, Öffentlich-rechtliche Hemmnisse für die Einführung des elektronischen Zahlungsverkehrs, in: Holznagel/Hoeren, Rechtliche Rahmenbedingungen des elektronischen Zahlungsverkehrs, 1999, S. 39 ff. sowie die anderen Beiträge in diesem Band.

3.5 Technische Voraussetzungen und Probleme [Autor: Berthold Weghaus (TÜViT)]

E-Commerce als Optimierung von Geschäftsabläufen ist ein Entwicklungsprozess, der durch das Zusammenwachsen traditioneller Unternehmensanwendungen und neuer Internet-Technologie geprägt ist. Dieser Prozess beinhaltet idealer Weise fünf Schritte:

1. Zugang zum Internet,
2. Präsenz im Internet,
3. Integration bereits bestehender Anwendungen in das Internet,
4. vertrauensbildende Maßnahmen und
5. Geschäfte mit E-Commerce im Internet.

Diese Schritte bestimmen dann auch die notwendige informationstechnische Ausstattung, insbesondere auch den Rahmen für die Sicherheit.

Sobald die genannten fünf Schritte absolviert sind, kann E-Commerce betrieben werden. Hierbei lassen sich vier Phasen im Ablauf unterscheiden:

1. Information erfolgt durch elektronische Produktkataloge.
2. Vereinbarung enthält die Preisermittlung und die Kaufvereinbarung.
3. Festsetzung beinhaltet den Zahlungsverkehr, die Aus-/Zulieferung der Ware sowie bezogene Versicherungsleistungen.
4. Nachbearbeitung umfasst die Kundenunterstützung sowie die Bearbeitung von Reklamationen, Garantieleistungen usw.

Zur Zeit reduziert sich E-Commerce jedoch noch vielfach auf den reinen Zahlungsverkehr, und auch in dieser Phase sind noch einige Probleme zu lösen. Grundsätzlich muss beim elektronischen Zahlungsverkehr zwischen E-Banking und E-Money unterschieden werden. Ersteres dient zur Tätigung von Bankgeschäften wie beispielsweise Homebanking (HBCI), letzteres zur Bezahlung von Waren und Dienstleistungen über offene Netzwerke (SET, Geldkarte usw.). Auf beide Zahlungsverkehrsarten ist oben bereits eingegangen worden, sie werden deshalb an dieser Stelle nicht weiter erörtert.

3.5.1 Anforderungen an elektronischen Wirtschaftsverkehr

Grundsätzlich gibt es eine ganze Reihe von Anforderungen an den elektronischen Wirtschaftverkehr. Dazu gehören die Rechtssicherheit, eine bestimmte Robustheit der Sicherheitsinfrastruktur sowie die Begrenztheit und gerechte Verteilung der verbleibenden Risiken (Restrisiko). Zu den im engeren Sinne sicherheitsrelevanten Anforderungen, die durch kryptographische Verfahren gelöst werden können, zählen das Erkennen und Verhindern von Manipulationen und Maskeraden, das Ausspähen von Geheimnissen, das Abstreiten von Handlungen, das Abfangen und Unterdrücken von Nachrichten sowie das Wiedereinspielen von Nachrichten.

Grundlage der Rechtssicherheit ist die technische Sicherheit der Endgeräte und des Datentransfers via Internet. Das Ziel muss sein, ein Sicherheitsniveau für das gesamte

System zu erreichen, das mit dem gewöhnlichen Geschäftsverkehr vergleichbar ist. Das implementierte Sicherheitsniveau sollte überprüfbar und von neutralen Instanzen bescheinigt sein[120]. Zum Schutz vor Gefahren auf den unsicheren Kommunikationswegen lassen sich zahlreiche Protokolle einsetzen. Gemeinsam ist allen, dass sie ihre Sicherheit im Kern durch starke Kryptoverfahren beziehen. Die Nutzer dieser Protokolle sind meist in eine Sicherheitsinfrastruktur eingebunden, die sich auf Trust Center als Zertifizierungsstellen für die verwendeten Schlüssel stützt. Jede Verwendung derartiger kryptographischer Verfahren setzt beim Benutzer eingebundener Endgeräte ein hohes Maß an Sorgfalt bei der Aufbewahrung und Anwendung der eingesetzten Schlüssel voraus. Die in den Endgeräten hierfür zuständigen Systemanteile sind hiernach als besonders sicherheitskritisch einzustufen.

Lokale Maßnahmen reichen dennoch allein nicht aus; sie müssen in den Rahmen einer globalen Sicherheitsinfrastruktur gestellt werden.

Eine Vielzahl von Gefährdungen bedrohen ein E-Commerce-System. Einige davon sind augenfällig, andere in der konkreten Implementierung verborgen, einige sind überhaupt nur Experten verständlich. Dementsprechend können Angriffe auf das System aus den verschiedensten Richtungen erfolgen.

Grundsätzlich sollte beachtet werden, dass viele Gefährdungen und damit die resultierenden Sicherheitsmaßnahmen auch von der Größe, der Art und dem Ansehen der Unternehmen, die E-Commerce betreiben, abhängen. Ein kleines oder mittleres Unternehmen setzt in der Regel Standardsoftware für seinen Internetauftritt ein, eine große Organisation primär proprietäre Software. Wenn bei Standardsoftware Sicherheitslücken auftreten, sind diese sehr schnell sehr vielen bekannt. Server mit Standardsoftware können daher von vielen angegriffen werden, weil dies keinen hohen intellektuellen Aufwand erfordert. Selbstentwickelte und/oder weiterentwickelte Software enthält statistisch genauso viele Fehler, diese muss ein Angreifer aber selbst herausfinden. Angriffe auf Server mit proprietärer Software sind daher anders motiviert.

Welchen Handlungsbedarf die diversen Bedrohungen für ein konkretes E-Commerce-System erfordern, hängt davon ab,

1. für wie wahrscheinlich der Eintritt gehalten wird,
2. welche Schäden dadurch verursacht werden können,
3. wie aufwendig die Durchführung eines entsprechenden Angriffs ist,
4. wie hoch das Entdeckungsrisiko für einen Angreifer ist.

Der erforderliche Sicherheitsgrad hängt nicht zuletzt von den ökonomischen Rahmenbedingungen ab. Wie viel Sicherheit angemessen ist und welche Sicherheitsmaßnahmen dafür umgesetzt werden müssen, richtet sich unter anderem nach der Höhe der Zahlungsbeträge, den angebotenen Waren und den vorhandenen Kenntnissen über die Kunden. Letztlich ist auch das angestrebte Sicherheitsniveau immer eine Frage der Wirtschaftlichkeit, also der Bezahlbarkeit der daraus resultierenden Maßnahmen.

120 Mögliche Methoden sind: ITSEC, CC oder das dedizierte TÜViT-Prüfverfahren auf der Basis operationalisierter Sicherheitsanforderungen des Zentralen Kreditausschusses (ZKA)

Auf der anderen Seite sollte aber auch klar sein, dass eine hundertprozentige Sicherheit nicht erreichbar ist. Auch bei bestmöglichen Sicherheitsmaßnahmen wird es beim E-Commerce immer Restrisiken geben.

3.5.2 Anforderungen an E-Commerce-Systeme

Die Anforderungen an E-Commerce-Systeme lassen sich mehreren Bereichen zuordnen:

1. Absicherung der Kommunikation,
2. Überprüfung der Identität der Kommunikationspartner,
3. Sicherheit der Komponenten (Endgerätesicherheit),
4. Absicherung des Benutzers,
5. Kundenhardware und -software,
6. Verhaltensregeln für Kunden,
7. Generelle Sicherheitsanforderungen.

3.5.2.1 Absicherung der Kommunikation

Zur Absicherung der Kommunikation zwischen den beteiligten Parteien müssen folgende Sicherheitsziele erreicht werden:

1. Manipulationen an den übertragenen Daten, insbesondere im Bereich Bestellung, Zahlung und Auslieferung, müssen erkannt, die Transaktionen bei Manipulation abgewiesen werden;

2. die Vertraulichkeit der übertragenen Daten, insbesondere von personenbezogenen Daten sowie Zahlungsverkehrsdaten, muss gewährleistet sein;

3. alte Transaktionsdaten dürfen nicht wiederverwendet werden können und

4. ein Ableugnen der Bestellung, der Zahlung oder der Auslieferung darf nicht möglich sein (Verbindlichkeit).

Um dies umsetzen zu können, lassen sich unter anderem folgende Maßnahmen einsetzen:

1. Integritätssicherung: Um sicherzustellen, dass die übertragenen Daten nicht zufällig oder absichtlich verfälscht worden sind, können die Daten mit einer kryptographischen Prüfsumme versehen werden. Hierzu können z.B. Message Authentication Codes, Hash-Verfahren oder Digitale Signaturen verwendet werden.

2. Verschlüsselung: Um die Vertraulichkeit der übertragenen Daten sicherzustellen, können sowohl symmetrische (z.B. DES, IDEA) als auch asymmetrische (z.B. RSA, elliptische Kurven) Verschlüsselungsverfahren benutzt werden.

3. Empfangsquittung: Will der Sender beweisen können, dass er dem Empfänger über das Kommunikationsnetzwerk Geld übermittelt hat, so braucht der Sender eine beweiskräftige Empfangsquittung des Empfängers. Dazu kann beispielsweise der

Empfänger aus den empfangenen Daten einen Hashwert bilden und diesen anschließend digital signiert als Empfangsquittung zurücksenden. Der Sender kann damit nachweisen, dass die Quittung vom Empfänger kommt und dass dieser die Quittung nur durch Kenntnis der übermittelten Daten erzeugen konnte. Also muss der Empfänger die Daten korrekt empfangen haben. Vergleichbares gilt für die Verbindlichkeit des Bestellens.

4. Verhinderung des Wiedereinspielens: Durch Verwendung von dynamischen Schlüsseln, Transaktionsnummern, Sequenznummern oder Zeitstempeln kann sichergestellt werden, dass wiedereingespielte Nachrichten als solche erkannt und abgelehnt werden können.

3.5.2.2 Überprüfung der Identität der Kommunikationspartner

Ein weiterer wesentlicher Punkt für die Sicherheit von E-Commerce-Systemen ist die Überprüfung der Identität der Kommunikationspartner. In offenen Kommunikationsnetzen kann man sich nicht darauf verlassen, dass Namensangaben korrekt sind. Daher muss die gegenseitige Authentifikation aller Systemkomponenten und gegebenenfalls auch von deren Benutzern gewährleistet sein. Hierzu werden üblicherweise Challenge Response-Verfahren eingesetzt.

3.5.2.3 Komponentensicherheit

Betreiber von E-Commerce-Systemen (Anbieter von Dienstleistungen) im Internet müssen beachten, dass ihre Gefährdungssituation sich von der eines Benutzers stark unterscheidet. Ein Anbieter muss einen Server betreiben, der im Internet bekannt und ständig verfügbar ist. Dieser Server kann gezielt angegriffen werden, um dem Anbieter Schäden zu verursachen. Daher muss der Anbieter eine offensive Absicherung seiner Rechner anstreben, der Kunde kann sich im Allgemeinen defensiv verhalten.

Als Anbieter müssen folgende Schutzziele erreicht werden:

1. Der Server muss ständig verfügbar sein, es sind nur kurzfristige Ausfallzeiten tolerabel.
2. Sämtliche Aktivitäten des Servers müssen revisionssicher nachvollziehbar sein.
3. Ein Missbrauch des Servers durch Innen- oder Außentäter muss ausgeschlossen werden.
4. Die Integrität und die Vertraulichkeit der verarbeiteten Daten müssen gewährleistet werden.

Um diese Schutzziele zu erreichen, ist eine Reihe von Maßnahmen notwendig, diese hier aufzuführen würde den Rahmen des Berichts sprengen. Deshalb werden hier die wichtigsten Maßnahmen kurz schlagwortartig skizziert. Zur Erläuterung sei auf die vielfältige Fachliteratur verwiesen:

1. Einsatz einer Firewall,
2. Access Control,
3. eingeschränkter Serverbetrieb,
4. ausfallsichere Systeme,
5. Hardware-Sicherheit,
6. Notfallvorsorge,
7. Datensicherheits- und Datenschutz-Audit,
8. DV-Revision und
9. geeignetes Personal.

3.5.2.4 Absicherung des Benutzers

Der Kunde im Online-Shop (typische Dienstleistung in einem E-Commerce-System) erwartet, dass er durch Benutzung bereitgestellter Software keinen Sicherheitsrisiken ausgesetzt wird. Beim Kunden kann kein tief gehendes Wissen über Sicherheitsrisiken und -maßnahmen vorausgesetzt werden. Er ist zwar für seinen Rechner und für die Endgerätesicherheit auf seiner Seite verantwortlich, ein Anbieter von E-Commerce-Dienstleistungen sollte ihn dabei allerdings durch Informationen oder Werkzeuge unterstützen.

1. Die Systemanteile, die beim Kunden installiert werden müssen, haben ein adäquates Maß an Sicherheit aufzuweisen.

2. Das System muss einfach zu bedienen sein, damit kein Benutzer gezwungen ist, sich bei sicherheitsrelevanten Teilschritten durch andere helfen zu lassen.

3. Alle Transaktionen (Bestellungen, Zahlungen usw.) müssen beweisbar, nachweisbar und fälschungssicher sein.

4. Das System sollte verlustsicher und fehlertolerant sein. Weder Systemabstürze noch Verbindungsunterbrechungen dürfen zu Geldverlusten für den Kunden führen.

5. Das System sollte bereits so konzipiert sein, dass Datenschutz für den Kunden gewährleistet ist. Es sollte eine weitestgehende Anonymität ermöglichen und nur ein Minimum an Informationen über den Kunden weitergeben.

Auch wenn vielfach das Schlagwort Anonymität verwendet wird, muss dies nicht immer heißen, dass Zahlungen völlig anonym verlaufen. Häufig wird unter Anonymität nur verstanden, dass der Händler die Kontendaten des Kunden nicht lesen kann und die Bank nicht die Bestellinformationen. Der Händler muss nicht den einzelnen Kunden identifizieren können, außer er braucht eine Lieferadresse, er muss dessen Zahlungsfähigkeit überprüfen können.

3.5.2.5 Kundenhardware und -software

Das notwendige Sicherheitsniveau kann durch Software alleine nicht erreicht werden. Wenn das jeweilige System die Speicherung von sensiblen Daten wie kryptographischen Schlüsseln, PINs oder virtuellem Geld beim Kunden erfordert, muss diesem dafür zusätzlich angriffsresistente Hardware zur Verfügung gestellt werden (Hardware-Software-Codesign). Dies können beispielsweise Chipkarten sein. Diese bieten außerdem den Vorteil, dass die Kunden damit sowohl von zu Hause als auch von wechselnden Einsatzorten aus online einkaufen können, falls die erforderliche Infrastruktur wie beispielsweise ein vertrauenswürdiger Chipkartenleser vorhanden ist.

Die Kundenhardware und -software sollte grundsätzlich die folgenden Sicherheitsanforderungen erfüllen:

1. Es dürfen keine Zahlungen ohne Zustimmung des Kunden durchgeführt werden können. Die Zustimmung kann hierbei implizit durch Eingabe eines Passworts bzw. einer PIN, der Nutzung eines biometrischen Merkmals und/oder einer Chipkarte gegeben werden (Wissen und Besitz). Dies verhindert unter anderem den unbefugten Zugriff aus dem Umfeld des Kunden.

2. Computer-Viren oder so genannte Trojanische Pferde dürfen keine Änderungen im Zahlungsverkehr vornehmen können. Insbesondere darf es grundsätzlich für Software nicht möglich sein, Zahlungsverkehr zu manipulieren oder eine Transaktion unbemerkt vom Kunden durchzuführen.

3. Ein Systemabsturz darf nicht zum Geldverlust führen. Das Produkt sollte eine Möglichkeit bieten, ein Recovery bzw. Backup der zahlungsrelevanten Daten durchzuführen.

4. Vertrauliche Informationen zum Zahlungsverkehr, wie beispielsweise Passwörter, PINs, Transaktionsnummern und/oder kryptographische Schlüssel, müssen sicher gespeichert sein, sodass nur der autorisierte Kunde darauf zugreifen kann.

5. Bei der Durchführung des Zahlungsverkehrs darf der Kunde nicht über die Höhe des Geldbetrags einer Transaktion getäuscht werden. Die Integrität der Daten muss gewahrt bleiben.

6. Sämtliche Transaktionen müssen nachvollziehbar gespeichert werden.

7. Um diese Ziele erreichen zu können, muss zunächst der Anbieter eines E-Commerce-Systems eine Reihe von Maßnahmen realisieren:

    a) Bereitstellen eines geeigneten Produkts: Bei reinen Software-Produkten muss der Kunde eine Vielzahl von sicherheitsrelevanten Konfigurationen und Vorgängen beachten. Erhält er zusätzlich dazu eine Hardwareergänzung, so können hierauf die kryptographischen Schlüssel und die geldwerten Informationen sicher und transportabel gespeichert werden.

    b) Qualitätssicherung des Produkts: Ebenso wie auf Anbieterseite sollten die Produkte des Kunden unabhängig auf ihre IT-Sicherheit hin untersucht werden.

c) Produktspezifische Aufklärung des Kunden: Dem Kunden sind aussagekräftige Unterlagen darüber zur Verfügung zu stellen, was unter Sicherheitsaspekten bei der Durchführung des Zahlungsverkehrs produktspezifisch zu beachten ist. Dazu gehören beispielsweise auch Hinweise, wie ein Browser sicher zu betreiben ist, oder die Empfehlung, keine ausführbaren Programme vom Internet zu laden. Über die Risiken beim Umgang mit Passwörtern und kryptographischen Schlüsseln sollte aufgeklärt werden. Informationen zum Datenschutz bzw. zum Umgang mit personenbezogenen Daten sind ebenfalls bereitzustellen.

d) Systemspezifische Aufklärung des Kunden: Da viele Kunden die für ihren Rechner notwendigen IT-Sicherheitsmaßnahmen nicht kennen, sollte der Anbieter dem Kunden hierüber Informationen bereitstellen.

3.5.2.6 Verhaltensregeln für Kunden

Für die Kunden muss das Risiko transparent und das verbleibende Restrisiko kalkulierbar sein. Sie müssen wissen, wie sie sich zu verhalten haben, damit ihnen durch die Benutzung der Verfahren keine Schäden entstehen. Dazu müssen sie einige Maßnahmen umsetzen, um über das Internet sicher E-Commerce betreiben zu können.

1. Beachtung der Sicherheitsempfehlungen: Der Kunde sollte die vom Anbieter bereitgestellten Informationen und Sicherheitsempfehlungen beachten. Sind diese nicht aussagekräftig genug, sollte er verständlichere oder ausführlichere Informationen einfordern.

2. Datensicherung: Der Kunde sollte von seinen Daten, insbesondere den finanzrelevanten, eine regelmäßige Datensicherung erstellen. Damit bleibt er im Falle von technischen Defekten oder mutwilligen Schäden arbeitsfähig.

3. Vermeidung von Computer-Viren: In jedem Fall sollte der Kunde sicherstellen, dass sein Rechner vor Computer-Viren, so genannten Trojanischen Pferden oder dubioser Software geschützt wird. Dazu zählt auch, keine ausführbaren Programme unbekannter Herkunft zu nutzen.

4. Sichere Aufbewahrung von Zugangsmitteln: Zugangsmittel wie Passwörter, PINs, TANs oder Chipkarten müssen sicher aufbewahrt werden. Sie sollten nach Möglichkeit nicht im IT-System gespeichert werden. Werden sie dokumentiert oder aufgeschrieben, sollten sie verschlossen aufbewahrt werden.

3.5.2.7 Generelle Sicherheitsanforderungen

Beim Aufbau eines E-Commerce-Systems ist sehr vielen Gefährdungen entgegenzuwirken. Dementsprechend muss eine Vielzahl unterschiedlichster Sicherheitsmaßnahmen umgesetzt werden. Damit diese gut aufeinander abgestimmt sind, hat der Betreiber Sorge dafür zu tragen, dass alle Sicherheitsmaßnahmen in einem umfassenden Sicherheitskonzept beschrieben sind. In diesem Sicherheitskonzept sind eine Vielzahl von einzelnen Komponenten sowie das Zusammenspiel dieser Komponenten zu betrachten. Dies reicht von der Frage nach der Fälschungssicherheit des elektronischen

Geldes bis hin zum Schlüsselmanagement. Entsprechend der „Natur“ dieser einzelnen Komponenten sind Maßnahmen organisatorischer, personeller, infrastruktureller und technischer Art zu treffen, um die angestrebten Sicherheitsziele zu erreichen. Hierbei sind folgende Aspekte wichtig:

1. Es sollten nur kryptographische Algorithmen eingesetzt werden, die heute und für die nächsten Jahre als stark genug angesehen werden können. Daher sollte beispielsweise nur noch Triple-DES eingesetzt werden. Wenn RSA benutzt wird, sollte mit einer Schlüssellänge von mindestens 1024 Bit gearbeitet werden.

2. Das System muss Kontrollmechanismen beinhalten, mit denen Attacken (z.B. Duplizieren von Werteinheiten) rechtzeitig erkannt und damit entsprechende Gegenmaßnahmen eingeleitet werden können. Auch hier müssen wiederum Datenschutzaspekte berücksichtigt werden; trotz Kontrollmechanismen darf es nicht möglich sein, Kundenprofile zu generieren.

3. Für die Benutzung von E-Commerce-Systemen muss dem Kunden sowohl Hard- als auch Software zur Verfügung gestellt werden. Dabei müssen beide Komponenten ein angemessenes Sicherheitsniveau bieten. Wenn das jeweilige System die Speicherung sensibler Daten beim Kunden erfordert, sollten diese in angriffsresistenter Hardware (Sicherheitsmodul in Form einer Chipkarte) gespeichert werden. Die Software sollte Selbsttests durchführen können, um Modifikationen durch so genannte Trojanische Pferde oder Viren verhindern zu können. Wenn geldwerte Informationen beim Kunden gespeichert werden, muss sichergestellt sein, dass ein Systemabsturz nicht zum Geldverlust führt.

4. Alle sicherheitsrelevanten Informationen müssen zuverlässig gegen Manipulation und unbefugten Zugriff geschützt werden. Zu den sicherheitsrelevanten Informationen zählen PINs und kryptographische Schlüssel ebenso wie Kreditkartennummern und Bestell- oder Zahlnachrichten. Diese Daten müssen in allen Systemkomponenten adäquat geschützt werden, also nicht nur bei der Übertragung, sondern auch auf allen beteiligten IT-Systemen.

5. Zur Erreichung der Sicherheitsziele ist es neben der Auswahl geeigneter Maßnahmen ebenso notwendig, diese sorgfältig umzusetzen und anschließend die Umsetzung gründlich und regelmäßig zu kontrollieren. Hierbei ist es insbesondere wichtig, dass diese Kontrollen durch unabhängige Stellen erfolgen. Die Sicherheitsuntersuchungen müssen nicht unbedingt auf Grundlage formaler Kriterien wie den ITSEC oder den Common Criteria erfolgen, aber sie sollten durch unabhängige, erfahrene Sicherheitsexperten durchgeführt werden. Untersuchungen auf Grundlage der ITSEC oder Common Criteria erleichtern aber allen Anwendern die Vergleichbarkeit der Ergebnisse mit anderen Produkten.

6. Angesichts der geltenden Verbindlichkeit der übermittelten Aufträge in chipkartengestützten Systemen müssen die technischen Komponenten und Teilsysteme des E-Commerce-Systems die Sicherheitsanforderungen der Kreditwirtschaft erfüllen. Die Sicherheitsanforderungen werden durch Systemeigenschaften, die Art der Systemsoftware und -hardware und den Betreib von Netzen praktisch umgesetzt. Ihre Einhaltung muss über alle Detailstufen der Architektur nachgewiesen werden.

3.5.3 Klassifizierung der einsetzbaren Protokolle und Standards

Auf dem Gebiet des E-Commerce gibt es eine Vielzahl von relevanten Protokollen und Standards. Um hier eine bessere Übersicht zu erreichen, werden die analysierten Standards in mehrere Gruppen unterteilt. Dabei wird eine grobe Klassifikation nach den anwendungsorientierten Verfahren einerseits und allgemeinen Basisstandards andererseits durchgeführt. Die Basisstandards sind in der Regel unabhängig von einem bestimmten Verfahren; andererseits nehmen anwendungsorientierte Verfahren typischerweise auf mehrere Basisstandards Bezug.

Anwendungsorientierte Verfahren sind in der Regel speziell für einen bestimmten Anwendungsbereich definiert worden. Diese Verfahren nehmen im Allgemeinen Bezug auf eine Reihe von Basisstandards aus dem Bereich Datenübertragung und Sicherheit sowie auf die zugehörigen Datenformate.

In der Gruppe *Datenformate* werden die jeweiligen Formate betrachtet, die bei der Übermittlung von Nutzdaten eine Rolle spielen.

Die Gruppe *Basisstandards Datenübertragung* umfasst alle relevanten Standards und Protokolle, die sich mit der Übertragung von Informationen zwischen zwei Anwendungen befassen. Diese Gruppe wird intern weiter grob nach den Schichten des OSI-Referenzmodells für offene Systeme strukturiert.

In der Gruppe *Basisstandards Sicherheit* werden die entsprechenden Protokolle und Verfahren betrachtet, die sich mit der Sicherung von Vertraulichkeit, Authentizität, Unveränderlichkeit und Nachweisbarkeit der übermittelten Daten befassen.

3.5.3.1 Anwendungsorientierte Verfahren

HBCI

Der HBCI-Standard, auf den sich bundesweit alle Banken und Sparkassen über ihre Dachverbände[121] geeinigt haben, wird zukünftig eine wesentlich problemlosere und kundenfreundlichere Durchführung von Bankgeschäften aller Art ermöglichen, wie z.B. Überweisungen, Kontoinformationen, Daueraufträge, Wertpapieraufträge und dergleichen mehr. Zudem vereinfacht der neue Standard den direkten elektronischen Dialog zwischen dem Kunden und seinem Kreditinstitut. Mit HBCI steht ein weit entwickelter Multibankingstandard zur Verfügung, der Transaktionen und die sichere Übertragung zwischen dem Kunden und der Bank regelt.

Die elektronische Signatur beweist, dass die HBCI-Nachricht des Kunden mit den darin enthaltenen elektronisch unterschriebenen Daten auf dem Übertragungsweg nicht verändert wurde (Integrität). Bei eingereichten Aufträgen ist es auch wichtig, dass die Herkunft eindeutig nachgewiesen werden kann (Nichtbestreitbarkeit). Dies wird ebenfalls durch die jeweilige elektronische Signatur garantiert. Erst nachdem die Bank die Signatur erfolgreich überprüft hat, wird ein Auftrag angenommen.

---

121 HBCI wird gefördert durch: Bundesverband deutscher Banken e.V., Deutscher Sparkassen- und Giroverband e.V., Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V. und Bundesverband öffentlicher Banken Deutschlands e.V.

Die Verschlüsselung stellt sicher, dass die gesamte Nachricht unleserlich gemacht wird, sodass diese niemals von Unbefugten eingesehen werden kann (Vertraulichkeit). Einer der möglichen Angriffe in einem offenen System besteht darin, Daten auf einer Leitung abzuhören und die gespeicherte Information wiederholt einzuspielen. So könnte beispielsweise eine Überweisung eines Kunden gegen dessen Willen mehrfach ausgeführt werden. Um dies zu verhindern, wurde in HBCI ein Verfahren zur Doppeleinreichungskontrolle spezifiziert, welches zum einen den Missbrauch ausschließt und zum anderen die Flexibilität des Kunden in keiner Weise einschränkt (Validität).

Auch wenn HBCI ein Höchstmaß an Sicherheit bieten wird, kann dennoch kein Kunde aus seiner Sorgfaltspflicht im Umgang mit den Schlüsselmedien (Schlüsseldiskette oder Chipkarte) entlassen werden. Im Gegenteil, den Schlüssel für die Sicherheit seines elektronisch geführten Kontos hat zukünftig jeder selbst in der Hand. Er muss die Verantwortung wahrnehmen, da an dieser Stelle die Möglichkeit der Banken endet, Missbrauch zu verhindern.

Open Financial Exchange (OFX)

OFX wird in einem Firmenkonsortium mit Microsoft, Intuit und CheckFree und adressiert den Bereich Electronic Banking für Homebanking, schließt aber explizit auch das Firmenkunden-Banking mit ein.

Die aktuelle Version 1.5 vom 3. April 1998 kann unter der WWW-Adresse www.ofx.net bezogen werden. Die Datenformate sind in einem OFX-spezifischen SGML-Derivat angelegt.

OFX bezieht sich auf folgende Bankaktivitäten:

1. Einholen von Umsatzauskünften,
2. Einholen von Kredit-Kartenumsätzen,
3. Kapitaltransfer, Überweisungen,
4. Elektronische Bezahlung,
5. Wertpapierhandel.

Mit OFX sollen nicht nur Banken, sondern auch Makler, Händler, Kreditkarten-Bearbeiter, Finanzberater und öffentliche Verwaltungen angesprochen werden.

Die Kommunikation zwischen dem Client und dem OFX-Server erfolgt stets über TCP/IP. Die einzelnen OFX-Transaktionen sind in HTML-Dokumente eingebettet.

OFX basiert auf einem so genannten Request- und Response-Modell. Der Request sowie die zugehörige Response werden in OFX als Nachricht bezeichnet. Die Nachrichten selbst sind bis auf eine Ausnahme wiederum in Transaktionen eingebettet. Eine Transaktion beinhaltet eine Transaction-ID, die auf Kundenseite die Zugehörigkeit der Response zu den abgesetzten Requests ermöglicht. Es können ein oder auch mehrere Requests (Batch-Mode) in einer OFX-Datei vorhanden sein. Der OFX-Server leitet alle Requests an die Bankenfachanwendung weiter und sendet lediglich eine Response an den Client zurück. Die Request sind in dem Format „Standard Generalized Markup Lan-

guage” (SGML) beschrieben. Das Batch-Modell erlaubt den Transfer der Requests über das Internet oder die Einreichung der OFX-Dateien über andere Transportverbindungen.

Für die Security auf unteren Schichten wird SSL eingesetzt. Geplant ist eine Security auf der Anwendungsebene auf Basis von PKCS#7.

SET

SET ist eine technische Spezifikation, die von EUROCARD/Mastercard und Visa entwickelt wurde, um die Sicherheit von Kreditkartenzahlungen in offenen Netzen wie dem Internet zu gewährleisten. Die Kreditkartenorganisationen wurden dabei von Microsoft, IBM, Netscape und anderen unterstützt. Bei der elektronischen Abwicklung von Zahlungen mittels SET kommen vornehmlich Leistungen in Betracht, die dem Konsumenten über Internet-Browser, CD-ROM oder in Papierform angeboten werden. Die Bestellung erfolgt in elektronischer Form. Das notwendige Bestellformular erhält der Karteninhaber vom Händler ebenfalls in elektronischer Form. Der Karteninhaber sendet die elektronisch unterschriebene Bestellung inklusive seiner Zahlungswünsche an den Händler. Der Händler überprüft über die Bank des Karteninhabers dessen Autorisierung.

Bei einer SET-Transaktion sind folgende Teilnehmer involviert:

1. Karteninhaber:
   Von ihm geht stets die Transaktion aus.

2. Bank des Karteninhabers:
   Die Bank des Karteninhabers stellt für diesen ein Konto bereit. Außerdem gibt sie die Kreditkarte an den Karteninhaber aus.

3. Händler:
   Der Händler bietet die Ware an und fordert den Rechnungsbetrag ein.

4. Bank des Händlers:
   Sie stellt dem Händler ein Konto bereit.
   Bei dieser Bank befindet sich meist die technische Infrastruktur zur Annahme der Transaktionen (SET-Gateway).

5. Die Kreditkartengesellschaft schützt das Warenzeichen der Kreditkarte und legt die Bestimmungen zur Abwicklung von Zahlungen mittels der Kreditkarte fest. Die Kreditkartengesellschaft kann ebenfalls auch als Bank des Karteninhabers auftreten.

6. Darüber hinaus könnten auch Provider die Transaktionen durchführen.

Eine SET-Transaktion geht stets vom Kunden, also dem Karteninhaber, aus. Die Bestellung des Kunden besteht aus zwei Teilen, der eigentlichen Bestellung und der Zahlungsanweisung. Beide Teile sind einzeln unterschrieben. Hierdurch kann der Händler die Zahlungsanweisung einzeln an die Bank zur Autorisierung senden, ohne die Bank über die Inhalte der Bestellung zu informieren. Der Händler wiederum erfährt die Kreditkartennummer des Käufers nicht.

SET verwendet zur Datenverschlüsselung SSL unter Verwendung von Zertifikaten. Der Standard beschreibt den Datenaustausch zwischen drei Teilnehmern an einer elektronischen Zahlung, nämlich Käufer, Verkäufer und Kreditkartenfirma. Im Zuge einer Transaktion wird die verschlüsselte Kreditkartennummer des Käufers nicht an den Verkäufer, sondern an den Kreditkartenherausgeber des Käufers übertragen, der die Transaktion bestätigt. Im Unterschied zu Electronic Banking sind also an einer SET-Verbindung drei statt zwei Teilnehmer beteiligt, wobei die übertragenen Daten im Wesentlichen aus der Kreditkartennummer des Käufers bestehen.

Aufgrund der intensiven Beteiligung der größten Kreditkartenunternehmen und Browser-Hersteller stellt SET den kommenden Standard für kreditkartenbasierte Zahlungen im Internet dar. Durch die im Vergleich mit Electronic Banking unterschiedliche Zielsetzung und Arbeitsweise steht aber zu erwarten, dass die Bedeutung von SET auf diese Art von Transaktionen beschränkt bleiben wird. Aus Sicht der Bank ist ein gemeinsamer Zugang sowohl für den elektronischen Zahlungsverkehr als auch für die elektronische Bezahlung wegen der nur einmal notwendigen technischen Ausstattung und der gemeinsam genutzten Sicherheitsvorkehrungen von Vorteil.

Open Trading Protocol

Das Open Trading Protocol (OTP) erarbeitet eine Reihe von Firmen und Bankorganisationen, um damit einen Standard für E-Commerce aufzubauen. Dafür wird von OPT ein Rahmen gesetzt, um E-Commerce-Systeme unabhängig vom elektronischen Zahlungsverkehr zu betreiben. Mit OPT werden keine E-Banking- oder E-Money-Verfahren ersetzt, sondern transparent eingebunden, z.B. HBCI, SET, OFX, Ecash, CyberCoin, Geldkarte usw.

Mit einer OTP-konformen Benutzerapplikation soll jeder Kunde bei jedem Händler einkaufen können, auch wenn dieser für den Zahlungsverkehr Applikationen anderer Firmen benutzt. OTP soll alle Zahlungs- bzw. Liefermodalitäten unterstützen: die Zahlung beim Bestellen oder erst nach Auslieferung an der Haustür oder elektronisch via Internet.

Standards Datenformate

In diesem Abschnitt wird eine Reihe von Standards für die Formatierung von Daten betrachtet, deren Einsatzbereich im Firmenkundengeschäft liegt.

DTA-Formate DTAUS und DTAZV

DTAUS beschreibt ein Datensatzformat für den Inlandszahlungsverkehr. Dieses Format kann zur Abwicklung des Zahlungsverkehrs über Magnetbänder, Disketten oder auch elektronische Verfahren dienen.

Mögliche Zeichensätze sind ASCII und EBCDIC, wobei bei dem letztgenannten bestimmte Felder numerisch gepackt sind.

Eine logische Datei darf *nur* Gutschriften oder *nur* Lastschriften enthalten.

Seine Bedeutung hat DTAUS beim Zahlungsverkehr über Datenträger sowie beim elektronischen Zahlungsverkehr im Rahmen des DFÜ-Abkommens und über HBCI.

DTAZV beschreibt ein Datensatzformat für den Auslandszahlungsverkehr.

Wie bei der DTAZV-Datei sind die Zeichensätze ASCII und EBCDIC möglich.

Wie auch das DTAUS-Format wird DTAZV beim Datenträgeraustausch, beim Zahlungsverkehr im Rahmen des DFÜ-Abkommens und über HBCI eingesetzt.

Das DTA-Format des Deutschen Kreditgewerbes wurde quasi vor dem EDI-Zeitalter konzipiert und ist daher wenig geeignet für eine integrierte, unternehmensübergreifende und automatisierte Weiterverarbeitung. So enthält das DTA-Format z.B. keinen strukturierten Nachrichtenteil für den Verwendungszweck und ist mit einer Länge von 13 x 27 Stellen den heutigen Anforderungen im kommerziellen Zahlungsverkehr nicht gewachsen. Häufig müssen die Angaben zum Verwendungszweck dem Begünstigten deshalb separat in Papierform zugestellt werden.

Für Inlands- und Auslandszahlungen müssen unterschiedliche Formate verwendet werden.

Die Zahl der elektronisch verfügbaren Finanznachrichten ist beschränkt. So fehlen beispielsweise Nachrichtentypen für das Anzeigen einzelner Umsätze oder eine international einsetzbare Lastschrift.

S.W.I.F.T.

S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunication) beschreibt international gültige Formate für bankenspezifische Transaktionen. S.W.I.F.T.-Dateien sind in ASCII oder EBCDIC kodiert.

S.W.I.F.T.-Formate werden nicht nur beim Electronic Banking zwischen den Banken eingesetzt; sie werden ebenfalls beim Zahlungsverkehr nach dem DFÜ-Abkommen oder mittels HBCI unterstützt. Möglich sind auch Mischformen, wie z.B. das Initiieren eines Zahlungsauftrags im DTAUS-Format und das Abholen der Tagesauszüge (Statements) im S.W.I.F.T.-MT940-Format.

EDIFACT

Electronic Data Interchange for Administration, Commerce and Transport, kurz EDIFACT, wurde von der UN, der Europäischen Kommission und Branchenvertretern als länder- und branchenübergreifender Standard zur weltweiten Kommunikation entwickelt. Damit ist die Basis für die Abwicklung sämtlicher Geschäftsvorfälle wie z.B. Bestellungen, Lieferstatusmitteilungen, Rechnungen, Zahlungsaufträge oder Zollformalitäten gegeben. Die Weiterentwicklung und Anpassung an Neuanforderungen der einzelnen Branchen erfolgt über nationale und internationale Normungsgremien und Benutzergruppen aus Handel, Industrie und Dienstleistungen.

Gerade für Unternehmen, die international tätig sind und/oder eine große Anzahl von unterschiedlichen branchenübergreifenden Geschäftsvorfällen tätigen, bietet sich EDIFACT als Gesamtlösung an. Durch die Nutzung eines einzigen Datenformats, das Nachrichten in strukturierter Form weiterleitet, eröffnen sich weitgehende Einsparungspotentiale.

Eine getrennte Abwicklung von Inlands- und Auslandszahlungen ist hier nicht notwendig, da EDIFACT diese in einem einheitlichen Format verarbeitet.

Gutschrifts- und Belastungsanzeigen im EDIFACT-Format können unabhängig vom Kontoauszug erstellt werden und ermöglichen eine zeitnahe und flexible Finanzdisposition.

Ein weiterer wichtiger Vorteil von EDIFACT ist die Möglichkeit, Mehrwertdienste, z.B. Services zur Protokoll-, Medien- und Formatkonvertierung, Ergänzungs- sowie Archivierungs- und Sicherheitsservices anzugliedern und damit aus dem Unternehmen auszulagern.

HTML-orientierte Formate (OFX)

Die Syntax des OFX-Protokolls ist stark an HTML angelehnt. Die Formatbeschreibung selbst basiert auf SGML (Standard Generalized Markup Language). Die OFX-Transaktionen (Requests und Responses) sind in HTTP-Protokollanweisungen eingebettet. OFX unterscheidet so genannte OFX-Header, OFX-Request und OFX-Responses. In einer OFX-Datei können mehrere Requests und Responses vorhanden sein. Weiterer Vorteil bei HTTP ist die Fähigkeit, verschiedene Objekte (Multiparts) in einer HTTP-Datei zu versenden. So ist es möglich, z.B. ein OFX-Objekt und eine JPEG-Graphik in einer HTTP-Datei zu übertragen.

Nachteil bei OFX ist die zurzeit fehlende Kompression der Daten.

ASN.1-orientierte Formate (SET)

SET-Nachrichten sind nach dem ISO/IEC und ITU-T Abstract Syntax Notation (ASN.1)-Standard aufgebaut und nutzen die Distinguished Encoding Rules (DER).

ASN.1 liefert eine eindeutige Definition für die Inhalte von Nachrichten, DER eine sichere Verschlüsselung und elektronische Unterschrift.

Die ASN.1-Notation schließt eine Sammlung von Typen ein, die hinsichtlich SET erweitert wurden, besonderen Restriktionen unterliegen und durch die jeweilige Anwendung überprüft werden.

Basisstandards Datenübertragung

Die analysierten Basisstandards im Bereich der Datenübertragung werden weiter grob nach dem Schichtenprinzip des ISO-Referenzmodells für offene Systeme unterteilt:

Die Übermittlungsschicht ist den OSI-Schichten 5-7 zugeordnet und bieten den Anwendungsprozessen allgemeine, hochwertige Kommunikationsdienste in verteilten Umgebungen wie Filetransfer, Electronic Mail und World Wide Web.

Die Transportschicht entspricht grob den Schichten 1-4 des ISO-Referenzmodells für offene Rechnernetze (OSI). Hierin sind alle Standards und Protokolle zusammengefasst, die der Basis-Übertragung von Daten über physikalische Netze, sowohl im lokalen Netz als auch im Weitverkehrsnetz, dienen.

File Transfer Access and Management (FTAM)

FTAM ist ein offener Standard der ISO (ISO 8571) und dient zur Verwaltung sowie zum Transfer von Dateien im heterogenen Rechnerverbund.

FTAM kommt besondere Bedeutung im öffentlichen Bereich und bei der Kommunikation zwischen Bank und Firmenkunden im Rahmen des DFÜ-Abkommens zu, aber auch bei der Kommunikation zwischen den Banken und den Landes-Zentralbanken im Rahmen der elektronischen Öffnung der Deutschen Bundesbank.

FTAM unterscheidet einen sogenannten Requester und Responder. Der Requester verhält sich stets aktiv, d.h., mittels Requester können Verbindungen zu einem Responder aufgebaut, Dateien versandt und abgeholt werden.

FTAM sorgt für eine sichere Datenübertragung, d.h., die Dateien werden vollständig und korrekt übertragen. FTAM verfügt über Restart- und Recovery-Eigenschaften. Kommt es zu einem DFÜ-Abbruch, so wird die Datei entweder komplett oder anhand von Check-Points teilweise wiederholt übertragen.

FTAM steht in engem Zusammenhang zu FTP, dessen Bedeutung im Internet-Umfeld liegt.

X.400

X.400 ist ein offener Standard der ISO/ITU. Er beschreibt ein Message Handling System (MHS) ähnlich der analogen Briefpost. Die CCITT veröffentlichte 1984 die erste Reihe von Empfehlungen. Erweiterungen zu den Standards wurde 1988 und 1992 veröffentlicht. Die meisten auf dem Markt befindlichen Systeme unterstützen zumindest den 1988er-Standard. Das Modell eines Nachrichtenübermittlungssystems gemäß X.400 besteht aus einem Message Handling System (MHS) und seinen Benutzern. In diesem Modell kann der Benutzer entweder eine Person oder eine Anwendung sein. Benutzer sind entweder direkte Benutzer oder Anwendungen, welche auf das System mittels eines User Agents (UA) zugreifen.

Das Message Handling System selbst besteht aus einer Anzahl von funktionalen Elementen. Diese Elemente sind:

1. Message Transfer System (MTS),
2. Message Store (MS),
3. User Agent (UA),
4. Message Transfer System (MTS).

Das MTS stellt einen zuverlässigen, verbindungslosen Übermittlungsdienst zwischen Benutzern zur Verfügung, der Nachrichten nach dem „Store-and-Forward-Prinzip" übermittelt. Eine von einem Benutzer (Originator/Absender) abgesendete Nachricht wird durch das MTS transportiert und an einen oder mehrere Benutzer (Recipients/Empfänger) ausgeliefert.

Da das MTS aus mehreren Message Transfer Agents (MTAs) besteht, die innerhalb des X.400 Netzwerks verteilt sind, kann die Übertragung einer Nachricht daraus bestehen, dass sie solange von einem MTA zu einem anderen transferiert wird, bis jener MTA erreicht ist, der den Empfänger bedient.

Eine Nachricht besteht aus zwei Teilen, Envelope und Content. Im Envelope sind all diejenigen Informationen enthalten, die für die Vermittlung und Weiterleitung notwendig sind. Der Content stellt die Benutzerdaten dar, die in der Nachricht enthalten sind. Es gibt unterschiedliche Inhaltstypen (Content types) für verschiedene Arten von Nachrichten. Die Übertragung einer Nachricht selbst ist dabei vollkommen unabhängig von deren Inhaltstyp. Ein MTS ist daher nicht nur auf die Übertragung der definierten Inhaltstypen beschränkt; vielmehr lassen sich zusätzliche Inhaltstypen definieren und übertragen.

Mittlerweile hat der Standard bei der Anbindung der Benutzer an Bedeutung verloren. Hier sind es vor allem die Microsoft-Exchange-Clients, die durch proprietäre Zugriffsmechanismen auf die Exchange-Server zugreifen. Bei dem gesicherten Austausch von Nachrichten zeigt sich aber das Message Transfer System als weiterhin stark eingesetzter Standard. So basiert z.B. auch die Kommunikation zwischen den Microsoft Exchange Servern auf dem X.400-Standard.

Im elektronischen Zahlungsverkehr kommt X.400 z.B. im EDFACT-Umfeld Bedeutung zu, nämlich bei der Anbindung von Firmenkunden, die aus einer Mail-basierten Anwendung Zahlungsaufträge an die Bank leiten wollen.

Im Unterschied zu den Filetransfer-Verfahren wie FTAM, FTP, OFTP ist X.400 nach dem Store-and-Forward-Prinzip aufgebaut. Dies bedeutet: Der Absender liefert seine Nachricht zunächst an den nächsten Message Store, dieser wiederum an seinen angeschlossenen MTA und dieser wiederum an den nächsten MTA.

X.400 erlaubt mittels so genannter Gateways auch den Übergang zu den im Folgenden beschriebenen Standard-SMTPs.

Simple Mail Transfer Protocol (SMTP)

SMTP wurde 1979 als Standard für die Übertragung elektronischer Post definiert. Es regelt als Mitglied der TCP/IP-Protokollfamilie den Adressaufbau und Versand textbasierter Internet-Mail. Der Standard besitzt diverse Einschränkungen, die heute durch weitere Protokolle beseitigt wurden. So regelt SMTP lediglich den Versand zum Client, sieht jedoch keine Empfangsbenachrichtigung, garantierte Zustellung oder das Anhängen von Dateien vor.

SMTP ist heute der Standard für den Austausch elektronischer Post über das Internet. Dabei spielt der hierdurch geregelte Aufbau von Adressen (name@domain) die Hauptrolle, da zusätzliche Protokolle komfortablere Möglichkeiten wie die Verwendung von Zustellbenachrichtigungen vorsehen.

MIME (Multipurpose Internet Mail Extensions) ist eine Erweiterung zum SMTP-Standard, die es erlaubt, verschiedene Objekte, z.B. Graphiken und Video-Dateien, zu transferieren. Auch ist es hiermit möglich, mehrere verschiedene Objekte in einer Nachricht (multi-content) zu versenden.

SMTP steht in enger Beziehung zu den anderen Standards für die Übertragung von elektronischer Post wie POP und IMAP für die Regelung des Zugriffs auf E-Mail und ACAP für die Konfiguration diverser Zusatzoptionen, z.B. Adressverzeichnissen.

World Wide Web (WWW)

Der Ursprung von WWW liegt in einem akademischen Projekt des CERN (Centre Europeén de Recherches Nucléaires), des europäischen Zentrums für Hochenergiephysik in Genf.

1989 leitete dort eine Gruppe von Physikern ein Softwareprojekt in die Wege, das als globales, interaktives Informationssystem für die Hochenergiephysik dienen sollte. Zur gleichen Zeit wurden von NCSA (National Center for Supercomputing Applications an der University of Illinois at Urbana-Champaign) die ersten Implementierungen eines WWW-Servers begonnen. Diese sind die Basis vieler anderer Server-Implementierungen und -Portierungen. Ende 1990 war die erste zeilenorientierte WWW-Oberfläche auf einem NeXT-Computer verfügbar.

Das Ergebnis der darauf folgenden Entwicklungsarbeiten ist heute unter dem Namen World Wide Web (WWW) bekannt. Es ist mehr eine Initiative als ein Produkt. Ziel ist, mit Hilfe von Hypermedia-Informationssystemen universellen Zugang zu global verteilten „Dokumenten” zu gewähren.

Anfang 1993 wurden von verschiedenen Firmen WWW-Browser mit grafischer Oberfläche vorgestellt. Heute gehört WWW zu den beliebtesten Dienstleistungen des Internet, nicht zuletzt wegen der hohen Benutzerfreundlichkeit.

Die Pflege und Weiterentwicklung von WWW hat das W3-Consortium, das auch alle namhaften Industrievertreter beinhaltet, übernommen.

WWW unterscheidet die Protokolle HTTP und HTML:

1. HTTP (Hypertext Transfer Protocol) dient, wie der Name schon sagt, zum Transport der HTML-Informationen auf der Basis von TCP/IP und kann auch unabhängig von WWW verwendet werden. Charakteristika von HTTP sind z.B. die Adressierung über „Uniform Resource Locators" (URL) und die integrierten Cache-Funktionen, die eine (unstrukturierte) lokale Ablage von Daten auf dem Kundensystem erlauben.
   HTTP ist in der Version 1.1 seit Januar 1997 verfügbar.

2. HTML (HyperText Markup Language) ist der eigentliche WWW-Darstellungsstandard und besteht aus Formattags, die eine Strukturierung von Dokumenten ermöglichen. Mit Hilfe dieser Tags können zahlreiche Fremdformate, wie z.B. Graphiken, Bilder oder auch Java-Applets eingebunden werden. Im HTML-Sprachvorrat befinden sich auch die Hyperlinks, welche das Navigieren im gesamten WWW-Space erlauben, indem sie z.B. Textpassagen mit URLs verknüpfen.

Die Merkmale von WWW sind:

1. Einfache, plattformunabhängige Tag-Language (HTML) zur Formatierung von Text-, Bild- und Ton-Dokumenten;

2. Navigation auf der Basis von Hyperlinks (URL, Universal Resource Locator);

3. Einbindung von Fremdformaten für die Darstellung von Bild, Ton und Video;

4. Bearbeiten von Benutzereingaben (HTML-Forms) durch CGI-Scripts auf dem WWW-Server;

5. Einbindung spezieller Programmerweiterungen auf Basis von Java-Applets oder ActiveX-Controls, Plug-Ins oder Helper-Applications, die auf dem Kundensystem ausgeführt werden.

WWW besteht immer aus einem Client, dem so genannten Browser, und einem Server, dem so genannten Web-Server. Im Laufe der Entwicklung von WWW sind beide um folgende wesentliche Funktionen erweitert worden:

1. Java-Applets,
2. ActiveX-Controls,
3. CGI-Scripts,
4. Plug-Ins,
5. Helper-Applications.

WWW hat bereits im Homebanking-Bereich eine zunehmende Bedeutung erreicht. Hierzu trägt zum einen der Internet-Boom bei, zum anderen zeichnen sich Internet-Anwendungen gerade im Electronic Banking-Bereich durch besondere Benutzerfreundlichkeit aus.

Daneben hat die Web-Technologie weitere Stärken:

1. Hohe Verteilung der Anwendung auf Basis von Java und ActiveX. Der Kunde kann direkt die Anwendungen der Bank nutzen. Änderungen und Erweiterungen stehen den Kunden unmittelbar zur Verfügung.
2. Die Kundenreaktionen auf bestimmte Anwendungen und Angebote können gemessen und für strategische Entscheidungen im Marketing herangezogen werden.
3. Anwendungen können zentral erstellt und verteilt werden.

WWW steht im engen Zusammenhang mit anderen Standards zur Realisierung von Präsentationsebenen, z.B. CEPT. Die Stärken von WWW sind:

1. WWW-Protokolle werden, unabhängig vom derzeitigen Standardisierungsgrad, auf internationaler Ebene vereinbart.
2. Ein dynamisch geladenes Java-Applet wird immer aktuell abgerufen, d.h., es werden keine alten Versionsstände auf dem Kundensystem vorgehalten.
3. Java ist eine vollwertige, objektorientierte Programmiersprache. KIT ist ein Präsentationsstandard, der nicht weiter strukturierte Objekte unterstützt.
4. Die Entwicklungen im Bereich WWW und Java gehen aufgrund des großen Marktdrucks extrem schnell voran. Fehlerbehebungen und benötigte Weiterentwicklungen entstehen in rapidem Tempo.
5. Es bestehen konkrete Aktivitäten in der Verknüpfung von Java mit der existierenden Welt, z.B. durch JDBC für Datenbankzugriffe oder durch Zugriff auf CORBA-Objekte für die Realisierung verteilter Anwendungen.

Transmission Control Protocol (TCP)

TCP/IP (Transmission Control Protocol/Internet Protocol) ist das im Internet benutzte Kommunikations-Protokoll. Aber auch in der Unix-Welt ist es sehr verbreitet.

Internet entstand aus dem ARPANET, das in den USA „geboren“ wurde. ARPA steht für Advanced Research Projects Agency. Diese Behörde war eine Abteilung des DoD, des U.S. Department of Defense. Ihre Aufgabe bestand darin, den wissenschaftlich-technischen Fortschritt im US-Militärbereich voranzutreiben.

Das ARPANET – das Netzwerk der ARPA – nahm den Betrieb im Jahre 1969 auf. 1980 erstellten die Erfinder des ARPANET eine neue Architektur und das TCP/IP-Protokoll.

Die Internetprotokolle können, wie das ISO/OSI-Modell, ebenfalls in ein Schichtenmodell, mit allerdings nur vier Ebenen, eingeordnet werden.

Die Ebenen 1 und 2 des ISO/OSI-Modells werden im *Internet Protocol Stack*, wie das Internet-Modell auch genannt wird, durch die Netzwerkebene abgedeckt. Das zentrale Protokollpaar TCP/IP stimmt ziemlich genau mit den ISO/OSI-Ebenen 3 und 4 überein. In den höheren Schichten hingegen unterscheiden sich Internet Protocol Stack und

ISO/OSI-Modell stark voneinander. Die fünfte, sechste und siebte ISO/OSI-Ebene werden im Internet Protocol Stack durch eine einzige Schicht, die Prozess- oder Applikationsschicht, dargestellt.

TCP/IP hat mit dem Internet-Boom immer mehr an Bedeutung gewonnen und ist aus allen Bereichen der elektronischen Kommunikation über Rechner nicht mehr wegzudenken, so auch selbstverständlich im Bereich Electronic Banking.

Internet setzt sich aus zahlreichen Standards und Diensten zusammen, von denen im Folgenden einige wichtige aufgezeigt werden:

1. Das Internet Protocol (IP): Das IP ist unten gesondert beschrieben.
2. Das Internet-Adresssystem: Jeder Rechner im Internet braucht mindestens eine eindeutige 32-bit-Internet-Adresse (IP-Adresse). Es gibt fünf Typen, je nachdem, zu welchem Netzwerk ein Rechner gehört, jedoch spielen derzeit nur die so genannten Klassen A, B und C eine Rolle.
3. Domain Name System (DNS): DNS wurde geschaffen, um Rechnern statt den IP-Adressen auch logische Namen zuordnen zu können. Das DNS wird bei Umsetzung des logischen Namens in die IP-Adresse in Anspruch genommen. Der gesamte Namenbereich ist in Zonen unterteilt. Ein Domain Name Server verwaltet einen Teil der logischen Namen.
4. Das Transportprotokoll (TCP): Das verbindungsorientierte Transportprotokoll TCP ist im Internet auf Ebene 4 der Protokollhierarchie angesiedelt. Es dient als Basis für Anwendungen wie WWW, Telnet oder FTP, bei denen eine zuverlässige Übertragung der Daten gefordert wird. Es stellt eine bidirektionale Verbindung zwischen den Partnern her. Zuverlässig bedeutet dabei, dass die Datenübertragung gesichert erfolgt und die gängigen Sicherungsverfahren wie Sequenznummernvergabe, Prüfsummenbildung mit Empfangsquittungen, Quittungen mit Zeitüberwachung und Sliding-Window-Verfahren angewendet werden.
5. Das User Datagram Protocol (UDP): UPD ist als verbindungsloses Transportprotokoll einfacher gestaltet als TCP und steht für Dienste, die keine gesicherte Transportverbindung benötigen, oder für Dienste im sicheren LAN-Umfeld, bereit.

Internet Protocol (IP) und IPnG/IPv6

Das Internet Protocol (IP), auf der Netzwerkschicht (Ebene 3) angesiedelt, bildet zusammen mit dem Transmission Control Protocol (TCP) (Transportschicht) das zentrale Protokollpaar der Internet-Architektur. Die Hauptaufgabe des Internet-Protokolls ist das Adressieren von Rechnern sowie das Fragmentieren von Paketen der darüber liegenden Schicht. IP stellt also die Endsystemverbindung der Partnerrechner her. Der darüber liegenden Ebene (Transportschicht) bietet IP einen so genannten unzuverlässigen und verbindungslosen Dienst an. Wenn also, wie z.B. beim Dateitransfer, eine zuverlässige Übertragung gefordert wird, dann ist es Aufgabe eines der übergeordneten Protokolle (z.B. des Transportprotokolls), die Zuverlässigkeit zu gewährleisten.

Bei IPv6 handelt es sich um das Internet Protocol Version 6. Es wurde von 1992 bis 1994 entwickelt, um den Adressenengpass der bisherigen 32-bit-IP-Adressen zu beseitigen, und ist seit 1994 unter der Bezeichnung IPv6 spezifiziert. Die erweiterten Adressierungsmöglichkeiten sind notwendig, um dem sehr rasanten Anstieg der Nutzer im Internet gerecht zu werden.

IPv6 hat im Augenblick noch geringe Bedeutung, da seine Implementierung nur relativ langsam voranschreitet. Sollte sich aber der Adressenengpass des bisherigen IPv4 als tatsächlich bedeutsam herausstellen, so ist davon auszugehen, dass sich IPv6 sehr schnell durchsetzen wird, weil es bereits ein fertiger Standard ist. In einem Zeitraum von drei bis fünf Jahren dürfte es dann IPv4 verdrängt haben.

Basisstandards Sicherheit

Gerade beim E-Commerce müssen die Sicherheitsanforderungen bezüglich Integrität, Nichtbestreitbarkeit, Authentizität, Vertraulichkeit und Validität durch geeignete und auf dem neuesten Stand der Technik befindliche Sicherheitsmechanismen gewährleistet werden.

Zur Absicherung der Sicherheitsanforderungen werden in den folgenden Unterabschnitten geeignete Sicherheitsmechanismen vorgestellt.

EDIFACT Security

EDIFACT ist ein branchenübergreifender, internationaler Formatstandard für den Austausch von strukturierten Geschäftsdokumenten. Die EDIFACT-Normierung im Bereich des Zahlungsverkehrs und dokumentären Geschäfts gilt als weitgehend abgeschlossen. Die Vision, die hinter EDIFACT steckt, ist die elektronische Umsetzung von optimierten, unternehmensinternen und unternehmensübergreifenden Geschäftsprozessen mit einem möglichst hohen Automatisierungsgrad und der Aufbau einer vollständigen „electronic loop“ zwischen allen Beteiligten der Geschäftsprozesse. Diese Umsetzung erfordert die Analyse von Geschäftsprozessen mit ihren Organisationseinheiten, Kommunikationsflüssen, Funktionen, Daten und Ereignissen sowie die Zuordnung von EDIFACT-Nachrichten zu Geschäftsprozessen. Erst mit EDIFACT kann der elektronische Zahlungsverkehr in die „electronic loop“ zwischen allen Geschäfts- bzw. Kommunikationspartnern vollständig integriert werden.

Langfristig wird man auch die von den EDIFACT-Servern vorgenommene Konvertierung in die bankseitigen Inhouse-Formate DTA und S.W.I.F.T. über eine Anpassung der Anwendungssysteme der Bank mit durchgängigen EDIFACT-Kreisläufen ersetzen.

Bei der Übertragung dominieren derzeit FTAM, X.400 und proprietäre Lösungen. Eine wichtige technische Entwicklung wird die Übertragung von EDIFACT-Nachrichten über das Internet sein. Die für die Normierung im Internet zuständige Internet Engineering Task Force (IETF) hat hierzu bereits mit dem Internet-Draft RFC1767 einen ersten Vorschlag unterbreitet, EDIFACT-Nachrichten per Internet-Mail zu verschicken.

EDIFACT legt nicht die Verwendung konkreter Mechanismen und Verfahren fest. Es werden lediglich die Beschreibungsweisen, mit deren Hilfe man die zu nutzenden Mechanismen und Verfahren festlegen kann, normiert.

Zwei grundsätzliche technische Probleme für EDIFACT-Systeme bei der Verwendung von Kryptomechanismen zur Sicherung von Nachrichten wurden von den Autoren der Joint Security Working Group erkannt. Zum einen sind die Ergebnisse von kryptographischen Kalkulationen nicht unabhängig vom verwendeten Zeichensatz. Hierdurch werden gegebenenfalls eigens für die Berechnung bzw. Prüfung von z.B. Prüfsummen Konvertierungen notwendig. Zum anderen können durch die Zufälligkeit von kryptographischen Ergebnissen syntaktische Störungen von EDIFACT-Daten auftreten. Es erscheint jedoch bei näherer Betrachtung, als seien diese Probleme nicht alleine EDIFACT-spezifisch. In anderen Bereichen hat man eventuell lediglich noch kein ausreichendes Bewusstsein für derartige Schwierigkeiten. Man könnte die Tatsache, dass diese Probleme thematisiert wurden, ebenso gut als Ausdruck dafür werten, dass die „EDIFACT-Gemeinde“ mit Blick auf die technische Realisierung von EDI-Systemen und die dabei auftretenden Praxisprobleme möglicherweise einen Erfahrungsvorsprung besitzt.

Mit EDIFACT wurde erstmals ein branchenübergreifender, internationaler Formatstandard für den Austausch von strukturierten Geschäftsdokumenten mit definiertem Regelwerk und funktionsorientierten Nachrichten festgelegt, der auch noch weiterentwickelt wird.

Gerade im Hinblick auf den EU-Binnenmarkt, die Europäische Wirtschafts- und Währungsunion sowie die verstärkte Vernetzung internationaler Handels- und Finanzbeziehungen gewinnt eine einheitliche Kommunikation immer stärker an Bedeutung.

PEM

1985 begann die Entwicklung der PEM (Privacy Enhanced Mail) durch die „Privacy and Security Research Group (PSRG) mit dem Ziel, den E-Mail-Nutzern der Internet-Gemeinde Abhörsicherheit zu gewährleisten. PEM wird in den RFCs 1421-1424 spezifiziert. PEM stellt eine Vielzahl von Sicherheitsdiensten zur Verfügung:

1. Vertraulichkeit,
2. verlässlicher, authentischer Datenursprung,
3. verbindungslose Integrität und
4. Unterstützung bei unverwertbaren Daten mit Herkunftsbeweis.

Das Ziel von Privacy Enhanced Mail ist, Sicherheit für eine große Zahl von Anwendern bei der Übertragung von Mails zu gewährleisten. Aufgrund von Abwärtskompatibilität mit vorhandenen Mail-Transfersystemen wurde PEM dahingehend entwickelt, dass es im Internet als neuer Standard Fuß fassen kann. Im Gegensatz zu anderen Verfahren, die mehr Sachkenntnis vom User verlangen, ist PEM in ein Mail-System integriert, sodass es anwenderfreundlich ist.

Die PEM-Algorithmen unterstützen folgende Funktionen:

1. Nachrichtenintegrität,
2. Nachrichtenverschlüsselung und
3. Schlüsselübermittlung zum Nachrichtenentschlüsseln.

Die PEM-Standards legen keinen bestimmten Algorithmus fest, vielmehr verschaffen sie Anlagen zur Algorithmusidentifizierung (z.B. durch einen bestimmten Nachrichtenkopf).

Der spezifizierte Rahmen der PEM lässt verschiedene Konzepte zu, im Wesentlichen sind das die beiden Folgenden:

1. Das symmetrische Konzept benutzt einen (geheimen) Schlüssel, der beim Sender und Empfänger zum Kodieren und Dekodieren der Nachricht dient. Typischer Weise bietet der symmetrische Weg eine gute Performance (Leistungsfähigkeit), daher wird er zur Nachrichtenverschlüsselung benutzt.

2. Das asymmetrische Konzept benutzt ein Paar verschiedener, aber mathematisch verwandter Schlüssel. Dabei ist einer der Schlüssel öffentlich und einer privat (z.B. RSA). Der Sender verschlüsselt mit seinem privaten Schlüssel, der nur ihm bekannt ist.

Digitale Unterschriften können typischer Weise durch die Benutzung des asymmetrischen Konzepts in Kombination mit einer „one-way-hash function“ realisiert werden.

Digitale Unterschriften werden oft durch die Kombination einer „one-way-hash function“ mit einem asymmetrischen Algorithmus realisiert. Darunter versteht man eine Datenstruktur, die den öffentlichen Schlüssel an gewisse Attribute anbindet. Als Beispiel dient hier das X.509-Zertifikat, dieses knüpft den öffentlichen Schlüssel an einen Verzeichnisnamen und identifiziert den bzw. die Garanten für die richtige Anbindung. Die gesamte Datenstruktur ist dann noch – in ähnlicher Weise wie oben erklärt – digital unterschrieben.

Das PEM-System fördert den Gebrauch von Public-Key-Verschlüsselung zur Realisierung von Textverschlüsselung, Absenderidentifikation und Integrität. PEM akzeptiert alle Zertifikate, die nach CCITT X.509 gültig sind. Hinter CCITT X.509 verbirgt sich nicht ein bestimmtes Format, sondern ein ganzes Verfahren zur Zertifikation von Schlüsseln.

Im X.509 wird eine Certification Authority (CA) als eine Übereinkunft einer oder mehrerer User definiert, um Zertifikate zu erstellen und zu bestätigen. Dies ist keine semantische Übereinkunft, es geht lediglich um Übereinstimmung eines bestimmten Schlüssels mit einer bestimmten Identität.

Die PEM Spezifikation erlaubt die Benutzung der folgenden Algorithmen:

Data encryption	Data encryption DES
Data integrity	DES in ECB-Mode oder Triple-DES for encryption of hash values
Key encryption	RSA based on the PKCS 1 standard for asymmetric key management. DES in ECB-Mode oder Triple-DES for symmetric key management
Certificate	X.509 (1988)
Digital signature	RSA based on the PKCS 1 standard
Hash function	MD2, MD5

PEM definiert ein komplettes E-Mail-Sicherheitssystem mit einer öffentlichen Schlüssel-Infrastruktur, die skalierbar und für eine breite Anwendergruppe benutzbar ist.

PEM unterstützt keine binären Daten und speziellen Datentypen.

Die Anzahl der unterstützten kryptographischen Algorithmen ist begrenzt. Die Verschlüsselung basiert auf DES.

TeleTrusT Deutschland e.V. entwickelt eine E-Mail-Sicherheits-Spezifikation, genannt MailTrusT, die auf PEM basiert. Die MailTrusT-Spezifikation wird binäre Daten und spezielle Datentypen unterstützen und wird zusätzliche kryptographische Algorithmen erlauben.

Bei der Implementierung von digitalen Signaturen in neue Projekte ist, um Rechtsverbindlichkeit zu garantieren, die Konformität zum Signaturgesetz (SigG) bzw. zur Signaturverordnung (SigV) notwendig.

PGP

PEM hätte sich vermutlich als Standard durchgesetzt, hätte nicht zur gleichen Zeit (etwa ab 1987) der US-Amerikaner Phil Zimmermann sein Softwarepaket namens Pretty Good Privacy (PGP) auf den Markt gebracht. PGP erfüllt einen ähnlichen Zweck wie PEM-konforme Software, ist jedoch nicht PEM-konform. Unter normalen Umständen hätte kaum jemand das Außenseiter-Produkt PGP beachtet. Doch nichts in der Geschichte von PGP verlief normal, und so setzte sich dieses gegen den von der Industrie getragenen PEM-Standard durch. Die Gründe sind aus heutiger Sicht klar: PGP war den ersten PEM-Implementierungen qualitativ überlegen. PGP liegt ein konsequenterer Ansatz zugrunde: Beispielsweise verwendet PGP nicht den inzwischen „in die Jahre gekommenen“ DES, sondern das als deutlich sicherer geltende IDEA-Verfahren oder eine Dreifach-DES-VErschlüsselung (Triple-DES). Zudem werden bei PGP alle Informationen verschlüsselt, die nicht zur Übertragung notwendig sind. Bei PEM sind dagegen die digitale Signatur und andere Informationen auch nach der Verschlüsselung sichtbar.

PGP schreibt im Gegensatz zu PEM keine Trust Center vor, sondern ermöglicht jedem Anwender das Ausstellen von digitalen Zertifikaten. Der Vorteil dieses so genannten Web of Trust ist, dass es ohne spezielle Infrastruktur auskommt, auch wenn es in den

seltensten Fällen wirklich funktioniert. PEM sieht dagegen eine Hierarchie von Trust Centern vor, die es bis vor ein paar Jahren noch gar nicht gab.

PGP entspricht eher der Internet-Kultur als PEM: Während PEM zunächst nur eine umfangreiche Spezifikation darstellte, war PGP bereits ein Produkt, das alle verwenden konnten. Der Quellcode von PGP ist – im Gegensatz zu den meisten PEM-Implementierungen – öffentlich zugänglich und kann so von jedermann analysiert werden.

Der wichtigste Grund für den Erfolg von PGP war vermutlich der Wirbel, den PGP in der Öffentlichkeit verursachte. PGP-Programmierer Zimmermann wurde wegen eines angeblichen Verstoßes gegen die US-Exportbestimmungen für Kryptographie angeklagt (der Export von Krypto-Produkten ist in den USA gesetzlich stark eingeschränkt). Dabei entging er nur knapp einer Gefängnisstrafe. Dank seiner unnachgiebigen Haltung wurde er in Internet-Kreisen schnell zum Volkshelden. Eine bessere Werbekampagne hätte es kaum geben können.

S-HTTP

Ziel des S-HTTP-Protokolls war, Kompatibilität zu HTTP zu bewahren und dieses um Sicherheitsmechanismen zu erweitern. HTTP wird in den RFC 1945 spezifiziert. In Internet Draft Working Documents der Internet Engineering Task Force (IETF) vom Juli 1996 wird S-HTTP spezifiziert.

Standardisierungsinhalte

1. Kryptographische Mechanismen: Mit kryptographischen Mechanismen werden die im S-HTTP ermöglichten Sicherheitsdienste (Vertraulichkeit und Verbindlichkeit) erbracht.
    - Symmetrische Kryptosysteme: Als Beispiele für symmetrische Kryptoverfahren, die als Verschlüsselungsverfahren eingesetzt werden können, seien DES bzw. Triple-DES, FEAL und IDEA genannt.
    - Asymmetrische Kryptosysteme: Als Beispiele für asymmetrische Kryptoverfahren, die als Verschlüsselungsverfahren eingesetzt werden können, seien das RSA-Verfahren und das Verfahren von ElGamal genannt.
    - Hybridverfahren: Bei diesem Verfahren wird sowohl ein symmetrisches als auch ein asymmetrisches Kryptoverfahren als Verschlüsselungsverfahren eingesetzt.
2. Digitale Signaturverfahren: Als Beispiele für asymmetrische Kryptoverfahren, die als digitale Signaturverfahren eingesetzt werden können, seien das RSA-Verfahren, das Verfahren von ElGamal, das DSS-Verfahren und das Verfahren von Fiat und Shamir genannt. Bei einer Implementierung von digitalen Signaturen in neue Projekte ist für eine Rechtsverbindlichkeit die Konformität zum Signaturgesetz (SigG) bzw. zur Signaturverordnung (SigV) notwendig.

- Hash-Funktionen für digitale Signaturen: Zur Erstellung einer digitalen Signatur benutzt man so genannte (kryptographische) Hash-Funktionen. Eine Hash-Funktion h ist eine Funktion, die eine Zeichenfolge beliebiger Länge aufweist. Beispiele für Hash-Funktionen sind der MD5 (Message Digest Algorithmus), die Square-mod-n-Funktion, die SHS-Hash-Funktion und Hash-Funktionen auf der Basis des DEA.

3. Erweiterungen von HTML: Die Hypertext Markup Language HTML wird für S-HTTP um einige Aspekte erweitert. Das Konstrukt des Anchors (die Definition einer Verbindung zu einer anderen Seite) wird um die Möglichkeit der Definition von Optionen der Übertragung erweitert. Damit kann erzwungen werden, dass der Browser die Informationen zum Server nur verschlüsselt versendet. Er wird dem Server nicht anbieten, die Informationen unverschlüsselt zu übertragen. Ein neues Sprachelement, CERTs, ermöglicht die Übertragung von Zertifikaten innerhalb von HTML-Dokumenten zur späteren Verwendung durch den Browser. Die Verarbeitung der Zertifikate wird also der Anwendungsebene ermöglicht und nicht automatisch im Hintergrund durchgeführt.

Zur Realisierung der Sicherheitsdienste schreibt das Protokoll keine bestimmten Verfahren vor.

Die Mechanismen des SSL zur Identifikation von Server und Client sind ebenso wie die Einigung auf die zu verwendenden Verfahren beim S-HTTP von der Transportebene auf die Anwendungsebene verlagert worden:

1. S-HTTP bietet ein Sicherheitskonzept auf der Anwendungsebene.
2. S-HTTP verwendet das ungesicherte TCP als Transportmedium.

Die Sicherungsmodi und ihre Optionen werden von Server und Client ausgehandelt. Client und Server arbeiten hierbei gleichberechtigt, auch Clients können die sichere Übertragung initiieren.

Der Request des Client an den Server sollte digital signiert und verschlüsselt erfolgen. Die Signatur vermittelt dem Server Sicherheit über die Identität des Client und kann auf Grundlage dieser Informationen den Zugriff gestatten oder verweigern. Entsprechend kann sich der Client durch die Signatur des Server sicher sein, dass es sich tatsächlich um den Server handelt, der ihm das Dokument übermittelt.

Die kompletten HTTP-Transaktionen, in denen die Dokumentnamen vorkommen, werden verschlüsselt.

Obwohl WWW-Browser auch andere anwendungsorientierte Internet-Protokolle unterstützen, ist das am meisten verwendete Protokoll zwischen WWW-Clients und -Servern das Hypertext Transfer Protocol (HTTP). HTTP wird seit 1990 weltweit in der WWW Global Information Initiative verwendet. WWW nutzt es für hypermediale Seitenübertragung über das Netz.

S-HTTP hat bisher keinen wesentlichen Marktanteil. Außer für Open Marketplace Server, Vertrieb durch Open Market auf der Serverseite and Secure HTTP Mosaic von Enterprise Integration Technologies auf der Clientseite sind bisher keine kommerziellen Anwendungen bekannt.

Bei der Implementierung von digitalen Signaturen in neue Projekte ist für eine Rechtsverbindlichkeit die Konformität zum Signaturgesetz (SigG) bzw. zur Signaturverordnung (SigV) notwendig.

S/MIME

MIME (Multipurpose Internet Mail Extension) ist ein Nachrichtenformat für die Übertragung von Grafik und anderer Nicht-Text-Informationen mit E-Mail (Internet-Hintergrundprotokoll). MIME unterstützt einige vordefinierte Dateitypen wie GIF-Dateien, PostScript-Dateien, 8000 Hz gesampelte WAV-Audiodateien und auch multimediale Daten. Das PKCS-MIME Draft „S/MIME Message Specification: PKCS Security Service for MIME“ spezifiziert ein Format zur sicheren MIME-Übertragung.

Ziel von S/MIME (Secure MIME) ist, einen einheitlichen Weg zur Verfügung zu stellen, um sichere MIME-Daten zu senden und zu empfangen. Auf dem Internet MIME Standard basierend, liefert S/MIME die folgenden kryptographischen Sicherheitsdienstleistungen für elektronische Nachrichtenübermittlungsanwendungen:

Authentizität, Nachrichtenintegrität und Nichtabstreitbarkeit des Ursprungs (durch Benutzung der digitalen Signatur) sowie Vertraulichkeit und Datensicherheit (durch die Benutzung von Verschlüsselungsalgorithmen).

Standardisierungsinhalte

S/MIME Implementation Guide, Interoperability Profile, Version1 stellt Anforderungen und Empfehlungen zur Sicherstellung der Interoperabilität von S/MIME dar.

Die Sicherheit der Übertragung wird in PKCS-7 und -10 spezifiziert.

Security

Die S/MIME-Spezifikation erlaubt die Benutzung der folgenden Algorithmen:

Data encryption	RC2-40 bit CBC Mode (Default) DES-CBC-Mode Triple-DES (EDE3) CBC Mode
Key encryption	RSA according to PKCS 1. 512 bit modulus for export
Certificate	X.509 v 1
Digital signature	RSA according to PKCS 1 and PKCS 7
Hash function	MD2, MD5

Obwohl S/MIME kein Internet-Standard ist, konnte es auf dem nordamerikanischen Industriesektor Erfolge erzielen. Auf dem europäischen Markt gibt es nur wenige Anwendungen, und nordamerikanische Produkte mit Hochsicherheits-Verschlüsselungen können nicht exportiert werden.

Für die Übertragung von Grafik und anderer Nicht-Text-Informationen mit E-Mail bietet S/MIME ein Einsatzfeld.

Bei der Implementierung von digitalen Signaturen in neue Projekte ist für eine Rechtsverbindlichkeit die Konformität zum Signaturgesetz (SigG) bzw. zur Signaturverordnung (SigV) notwendig.

Mailtrust

In Deutschland ist neben S/MIME und PGP vor allem der vom Industrieverband Teletrust entwickelte E-Mail-Verschlüsselungsstandard Mailtrust von Interesse. Mailtrust entstand parallel zum 1997 in Kraft getretenen Signaturgesetz und ist auf dessen Anforderungen ausgerichtet. Mailtrust ist eine Erweiterung von PEM, die mit zusätzlichen Nachrichtenformaten und besseren kryptographischen Verfahren dessen Nachteile ausgleichen soll. Zu Mailtrust gehört auch die Spezifikation einer Schnittstelle zu einem Personal Security Environment (PSE), was im Normalfall eine Chipkarte ist. Chipkarten sind in den USA noch recht wenig verbreitet, weshalb dieser Teil bei amerikanischen Standards fehlt.

Aus Kompatibilitätsgründen unterstützt Mailtrust alle von PEM bekannten kryptographischen Verfahren. Zusätzlich sind Verfahren vorgesehen, die dem neuesten Stand entsprechen. So kann zur symmetrischen Verschlüsselung Triple-DES verwendet werden, die flexiblen X.509-Zertifikate der Version 3 werden jedoch nicht unterstützt.

Auch die PEM-üblichen Formatumwandlungen werden von Mailtrust unterstützt. Durch die Einführung neuer Nachrichtenformate kann aber auf diese Vorgänge verzichtet werden. Die Schnittstelle für Chipkarten entspricht dem PKCS#11-Standard. Mimen-Unterstützung bietet Mailtrust dagegen bisher nicht, was für den Einsatz im Internet durchaus einen Nachteil darstellt.

Mailtrust ist ein Standard, der auf die Situation in Deutschland zugeschnitten ist und von zahlreichen deutschen Unternehmen unterstützt wird. Die Chipkartenunterstützung und die Unterstützung einer Zertifizierungshierarchie entsprechen dem Signaturgesetz. Im Gegensatz zu S/MIME braucht sich Mailtrust auch nicht um das US-Exportverbot zu kümmern. Das große Problem des Mailtrust-Standards liegt darin, dass er eine deutsche Insel-Lösung darstellt. Mit einer Unterstützung durch die großen amerikanischen Software-Hersteller ist kaum zu rechnen. Es laufen daher derzeit Bemühungen, das S/MIME-Format in MailTrust mit aufzunehmen. Dies ist zwar technisch gesehen keine Ideallösung, da somit zwei völlig unterschiedliche Formate in einem Standard zusammengefasst werden. Aus Kompatibilitätsgründen gibt es jedoch keine Alternative. Langfristig könnte Mailtrust damit zu einer S/MIME-Erweiterung mutieren.

SSL

Die Entwicklung von SSL wird insbesondere von der Firma Netscape Communication vorangetrieben. Es liegt in der Internet Draft Version 3.0 vor. Die Arbeitsgruppe Trans-

port Layer Security WG im IETF-Security-Area möchte SSL schnell zu einem anerkannten Standard bringen.

Ziel von SSL ist, ein Protokoll zur Verfügung zu stellen, das die Datensicherheit auf einer Schicht zwischen HTTP und TCP/IP gewährleistet. Dieses Sicherheitsprotokoll, genannt SSL, ermöglicht Datenverschlüsselung, Echtheitsbestätigung von Servern und Nachrichtenintegrität für TCP/IP-Verbindungen.

Standardisierungsinhalte

Das SSL-Protokoll liefert eine Datensicherheit, die drei Grundeigenschaften besitzt:

1. Die Echtheit der Verbindung wird bestätigt. Eine Verschlüsselung wird nach einem Handshake benutzt, um einen geheimen Schlüssel zu definieren. Für die Datenverschlüsselung wird ein symmetrischer Schlüssel verwendet (DES oder Triple-DES).
2. Die Identität der Kommunikationspartner wird durch einen asymmetrischen Verschlüsselungsalgorithmus (z.B. RSA, DSS usw.) beglaubigt.
3. Die Verbindung ist vertraulich. Der Nachrichtentransport beinhaltet eine Nachrichtenintegritätsüberprüfung mit Hilfe einer MAC-Verschlüsselung. Sichere Hash-Funktionen (z.B. SHA, MD5 usw.) werden für MAC-Berechnungen verwendet.

SSL verwendet X.509-Zertifikate, deren Aufbau standardisiert ist. Damit können Zertifikate beliebiger Zertifizierungsstellen unterstützt werden, die sich an diesem Standard orientieren. Die Art des Zertifikats muss für den Schlüsseltauschalgorithmus der gewählten Schlüssel geeignet sein und ist im Allgemeinen ein X.509.v3- oder ein modifiziertes X.509-Zertifikat. Je nach zertifizierter Entität kann SSL zur Host-, Server- oder User-Authentisierung verwendet werden.

Security

Die SSL-Spezifikation erlaubt die Benutzung der folgenden Algorithmen:

Data encryption	RC4 with a 40 bit key (Export version), RC4 with 128 bit key, RC2 with 128 bit key, IDEA with 128 bit key, DES with 64 (56) bit key, Triple-DES with 192(168) bit key
Date integrity	MAC based on MD5 yielding 128 bits
Key encryption	RSA on the PKCS 1 Standard
Certificate	X.509 (1988)
Digital signature	RSA based on the PKCS 1 Standard
Hash function	MD5

Da SSL den Kern der Standardisierungsbemühungen einer eigenen Arbeitsgruppe, „Transport Layer Security“ der IETF-Security-Area, bildet, ist damit zu rechnen, dass es

schnell zu einem anerkannten Standard für gesicherte Verbindungen im Internet avancieren wird.

Bei der Implementierung von digitalen Signaturen in neue Projekte, ist für eine Rechtsverbindlichkeit die Konformität zum Signaturgesetz (SigG) bzw. zur Signaturverordnung (SigV) notwendig.

IPv6/IPSec

Im August 1995 wurden von der IESG entsprechende Internet Drafts als RFCs übernommen und als Proposed Standard in den IAB Standards Track eingebracht. Die Architektur von IPSP (IPv6/IPsec) ist in RFC 1825 beschrieben. IPv6 wird in RFC 1883 spezifiziert, in RFC 1884 die IPv6-Adressen.

Ziel von IPsec, gegenüber Ipv4, ist,

- IP-Header-Daten (Source and Destination Data) sowie Payload (User Daten) durch eine Signatur zu schützen und
- übergeordnete Protokolle (TCP, UDP) im IP-Datagramm verschlüsselt abzulegen.

Standardisierungsinhalte

- Authentification Heider (AH), schützt in erster Linie Integrität und Authentizität von IP-Paketen und ist in der RFC 1826 spezifiziert.
- Encapsulated Security Payload (ESP), schützt in erster Linie die Vertraulichkeit und ist in der RFC 1827 spezifiziert.

Standardalgorithmen sind in den RFCs 1828 und 1829 spezifiziert. Es handelt sich um DES im CBC-Mode für ESP sowie MD5 für AH.

Optional können auch alternative Kryptosysteme wie Triple-DES, CAST, SAFER, RC4 und IDEA eingesetzt werden.

Security

Im neuen Protokoll werden Sicherheitsmechanismen integriert sein, die eine Verschlüsselung von IP-Paketen ermöglichen. Somit kann nun auf der Ebene von IPv6 die Authentizität (Echtheitsüberprüfung) und Vertraulichkeit von Paketen gewährleistet werden.

Auf eine breite Einführung von IPv6 und der entsprechenden Sicherheitsdienste auf dieser Ebene wird man noch etwas warten müssen. Damit ist eine paketweise Prüfung der Daten auf dem Firewall-System nicht möglich. Durch den Einsatz von dynamischen IP-Filtermechanismen lassen sich die Risiken auf dieser Ebene jedoch minimieren. Anstatt jedes einzelne Paket zu prüfen (wie bei Ipsec), wird dann ein IP-Filter für genau diese Verbindung freigeschaltet.

4. Integration und Kooperation [Autor: Busso Grabow (Difu)]

4.1 Wechselwirkungen

Anwendungs-, Produkt- und Dienstleistungsinnovationen, wie sie im Rahmen der Projekte von *MEDIA*@Komm entstehen sollen, sind von einer Vielzahl von Rahmenbedingungen abhängig und Bestandteile eines äußerst komplexen „Echtzeit"-Wirkungsgefüges[122]. Echtzeit deswegen, weil durch die kontinuierliche Beschleunigung der Technikentwicklung, der Produktzyklen, der Veränderung von Markt- und Unternehmensstrukturen sowie Kooperationsbeziehungen in der Netzwerkgesellschaft entsprechende Reaktionen in äußerst kurzen Zeiten notwendig machen. Ursprünglich klare Grenzen werden immer „unschärfer" (z.B. zwischen Branchen, zwischen Produkten und Dienstleistungen, zwischen Konsument und Produzent), Ursache-Wirkungsbeziehungen werden uneindeutiger („Techniklösungen auf Problemsuche"[123]).

Die *MEDIA*@Komm-Projekte und die dort zu entwickelnden Lösungen, Produkte und Dienstleistungen sind hierfür prototypisch; Ausgangsannahmen und Entwicklungspläne, die in den Wettbewerbsbeiträgen enthalten waren, werden im Laufe der Umsetzung und nach Installation der Demonstrationslösungen vermutlich deutlich anders aussehen oder ihre ursprüngliche Gültigkeit verloren haben. Teilweise hinken auch die Rahmenbedingungen entsprechender Projekte (etwa die Förderinstrumente) in ihrer Geschwindigkeit und Ausrichtung den wirtschaftlichen und technischen Handlungsnotwendigkeiten hinterher. Dass die Beschleunigung und die Notwendigkeit des Handelns in Echtzeit in ihren Wirkungen auf die Gesellschaft durchaus ambivalent zu bewerten sind, ist offensichtlich[124]. Aus der vor allem ökonomisch begründeten Beschleunigungsfalle gibt es keinen Ausweg. Daher müssen auch die komplexen Rahmenbedingungen des Handelns in Innovationsprojekten wie *MEDIA*@Komm in ihrer eigenen Beschleunigungswirkung genauso wie in ihrer möglichen Bremserwirkung gesehen werden.

Die vielfältigen Wechselbeziehungen und die mannigfaltigen Rahmenbedingungen für die Entstehung von Innovationen und daraus erwachsenden neuen Wertschöpfungsprozessen sind in der CONDRINET-Studie der EU[125] am Beispiel eines „Interactive Content Value Web" dargestellt, also an einem System, in dem die Endnutzer von Online-Dienstleistungen zwar im Mittelpunkt stehen, das Verhältnis der Beteiligten (einschließlich der Endnutzer) und die Rahmenbedingungen aber ein äußerst komplexes Geflecht bilden. „Das Value Web ... soll anstatt einer statischen Struktur von Branchen, wie es vielleicht aussieht, ein dynamisches System darstellen und wettbewerbsbezogene Prozesse betonen, die auf Marktplätzen stattfinden. Die Segmente im Netz sollten nicht als starr aufgeteilt verstanden werden, sondern als sich ständig verschiebende «Anhäufung» von Aktivitäten, wobei die Anhäufungen, die am nächsten beieinander

122 Vgl. z.B. *Stan Davis und Christopher Meyer,* Das Prinzip Unschärfe: Managen in Echtzeit – Neue Spielregeln, Märkte, Chancen in einer vernetzten Welt, Wiesbaden 1998.

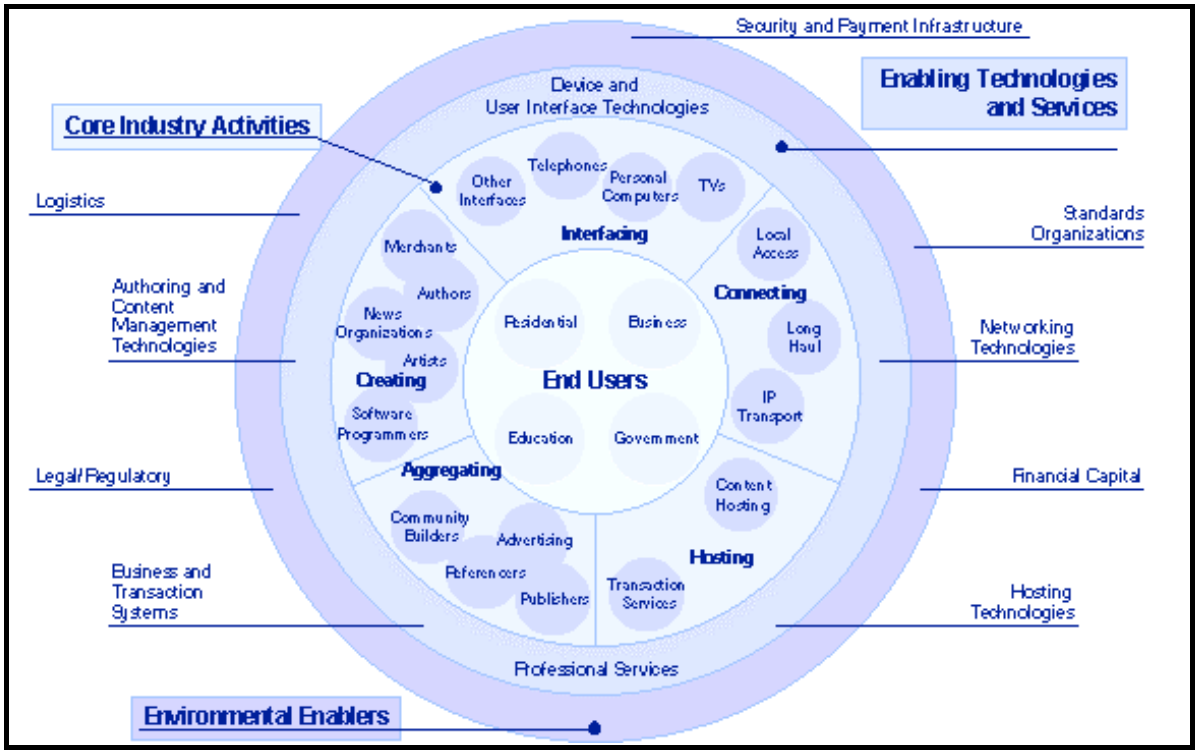
123 *Dieter Klumpp,* Marktplatz Multimedia. Praxisorientierte Strategien für die Informationsgesellschaft, Mössingen-Talheim 1996, S. 36.

124 Vgl. z.B. *Dietrich Henckel*, Geschwindigkeit und Stadt – die Folgen der Beschleunigung für die Städte, in: Dietrich Henckel, Holger Floeting, Busso Grabow u.a., Entscheidungsfelder städtischer Zukunft, Stuttgart u.a., 1997, S. 257-296 (Schriften des Deutschen Instituts für Urbanistik, Bd. 90).

125 http://www2.echo.lu/condrinet/Data/ge_sum.htm vom 21.10.1998.

sind, den stärksten Einfluss aufeinander haben."[126] Die Rahmenbedingungen („Environmental enablers") umfassen beispielsweise die rechtlichen Regelungen genauso wie die (technische) Sicherheits- und Zahlungsinfrastruktur, die ökonomischen Rahmenbedingungen (Finanzen, Logistik) oder die nationalen und internationalen Normen und Standards.

Abbildung: Beziehungsgeflecht und Rahmenbedingungen von Online-Dienstleistungen*



* Quelle: Gemini Strategic Research Group, Gemini Consulting, in: CONDRINET-Studie (Content und Commerce Driven Strategies in Global Networks), [http://www2.echo.lu/condrinet/Data/Ger/Chapters/Ge_Ch_1.htm] (Titel der Abbildung im Original „Interaktives Content Value Web").

Diese Rahmenbedingungen korrespondieren in vielerlei Hinsicht auch mit den individuellen und projektbezogenen Innovationshemmnissen bei den beteiligten Partnern der Dienstleistungs- und Produktinnovationen. Diese Hemmnisse sind – speziell für den IuK-Sektor – vielfältig, gelten nicht nur für private Unternehmen, sondern in übertragener Form auch für den öffentlichen Bereich und finden sich in allen Dimensionen, die auch im CONDRINET-Projekt aufgeführt sind.

126 http://www2.echo.lu/condrinet/Data/Ger/Chapters/Ge_Ch_1.htm.

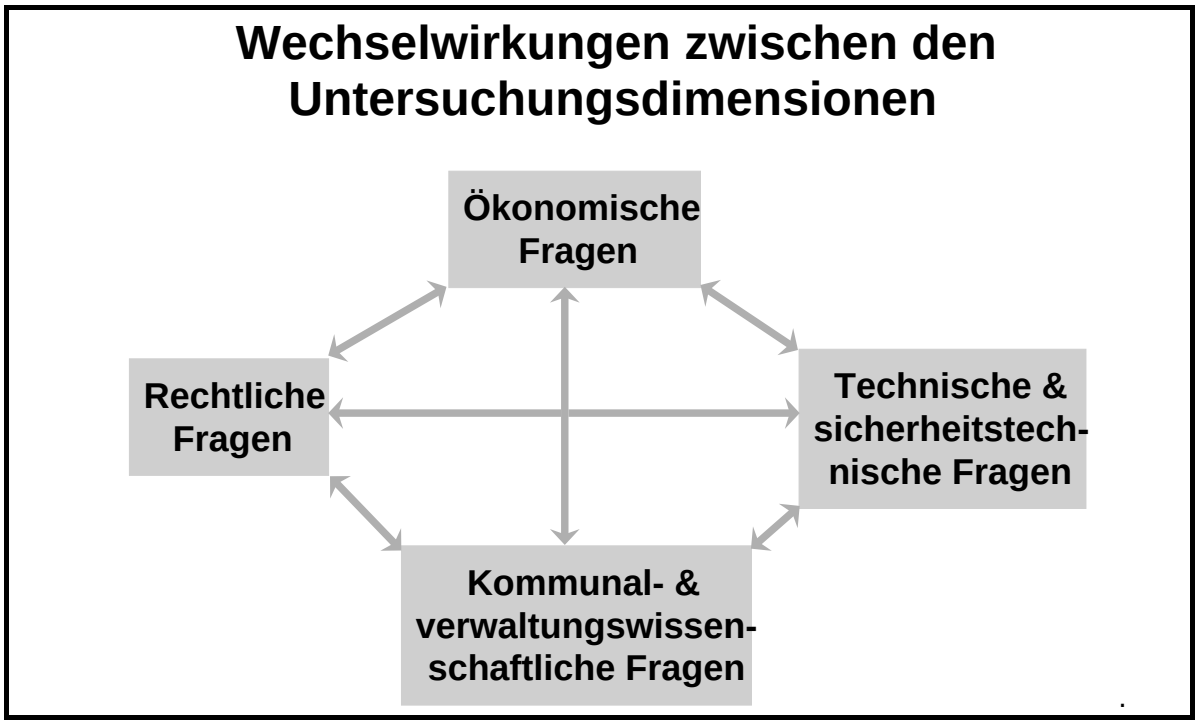
Übersicht: Art der Innovationshemmnisse*

Marktrisiken • Durchführbarkeitsrisiko • Risiko bzgl. Marktchancen • Kostenrisiko • Risiko langer Amortisationsdauer • Risiko leichter Kopierbarkeit • Schwere Vorhersagbarkeit der Kosten
Finanzierungsrestriktionen • Eigenkapitalschwächen • Fehlendes Fremdkapital
Rechtliche und bürokratische Hemmnisse • Lange Verwaltungs- und Genehmigungsverfahren • Gesetzgebung und rechtliche Regelungen
Unternehmensinterne Restriktionen • Mangel an Fachpersonal • Mangel an technischer Ausstattung • Nicht genügende Ausgereiftheit • Unternehmensinterne Widerstände

* Quelle: Darstellung nach *Georg Licht u.a.*, Innovationen im Dienstleistungssektor. Empirischer Befund und wirtschaftpolitische Konsequenzen, Baden-Baden 1997, S. 65, zitiert in: *Konrad Faust u.a.,* Tertiarisierung und neue Informations- und Kommunikationstechnologien, ifo Institut für Wirtschaftsforschung, München 1999, S. 153 (ifo studien zur strukturforschung 28/III).

Gemäß der oben genannten Rahmenbedingungen rechtlicher, (sicherheits-)technischer und ökonomischer Art einschließlich der Standards und Normen – die jeweils für sich genommen und in ihrer Vernetzung wichtig sind – ist auch die Begleitforschung organisiert. So sind im Konsortium fachliche Experten zu den jeweiligen Themenbereichen am Projekt beteiligt; das Expertenwissen wird möglichst eng verflochten. Dadurch lassen sich die Wechselbeziehungen der elementaren Rahmenbedingungen herausarbeiten (vgl. Abbildung).

Abbildung: Wechselwirkungen zwischen den Untersuchungsdimensionen*



*Quelle: Eigene Ausarbeitung.

Genauso lassen sich die möglichen Zielkonflikte innerhalb der fachwissenschaftlichen Untersuchung deutlich machen. Einige derartige Konflikte deuten sich bereits an:

- Hohe Sicherheitsstandards erhöhen tendenziell die Kosten von Online-Anwendungen.
- Die Infrastruktur und vorhandene Geschäftsprozesse in Kommunalverwaltungen sind bisher kaum für Internet-Anwendungen geeignet und erfordern erhebliche Investitionen in Technik und Organisation, die bei den beschränkten kommunalen Ressourcen nur schwer zu leisten sind.
- Rechtliche Regelungen etwa zur Anwendung der digitalen Signatur berücksichtigen technische Umsetzungshemmnisse und -probleme zu wenig; allerdings versucht man gerade in diesem Rechtsbereich durch die vergleichsweise schnelle Novellierung der Gesetze und Verordnungen solche Anpassungsprobleme klein zu halten.
- Der Nutzen kommunaler Online-Anwendungen entsteht vor allem bei den Bürgern und den Unternehmen, die Kosten fallen vor allem auf Seite der Kommunen an.
- Gesetzliche Regelungen setzen aus Sicht des Gesetzgebers wünschenswerte Normen, die aus Kosten- oder Handhabbarkeitsgründen nicht „marktfähig“ sein können.
- Das Normengerüst von Verwaltungsgesetzen und -vorschriften, Datenschutzregelungen und anderen rechtlichen Rahmenbedingungen engt die Möglichkeiten der Kommunen, kunden- und serviceorientierte Online-Verfahren einzusetzen, erheblich ein.

4.2 Kooperation und Zusammenführung von Kompetenzen

Aufgrund der Komplexität der Zusammenhänge, des Ineinandergreifens verschiedener Disziplinen sowie der Konvergenz der Branchen, Sektoren und Handlungsbereiche ist, wie oben beschrieben, die Zusammenführung vom Kompetenzen für das Gelingen solcher komplexer IuK- und Online-Projekte, wie sie in *MEDIA*@Komm realisiert werden sollen, ausgesprochen wichtig. In der Grundkonstruktion des Wettbewerbs war dieses Zusammenwirken verschiedener Kompetenzen, von öffentlichem Sektor, privaten Unternehmen, Intermediären und Bürgern, ja bereits angelegt.

Hinzu kommt, dass im Zuge der Technikentwicklung, der Branchen- und Aufgabenkonvergenz und bei verschwimmenden Grenzen neue Intermediäre in die Aushandlungs-/Geschäftsprozesse sowie in die Wertschöpfungsketten und -pools eingebunden werden[127]. Beispiele hierfür sind neue Dienstleister, wie etwa Sicherheits-, Informations-, Kommunikations- oder Interaktionsdienstleister. Derartige neue Intermediäre spielen in den *MEDIA*@Komm-Projekten eine wachsende Rolle.

Kooperation und die Zusammenführung von Kompetenzen sind aber nicht nur in den Projekten selbst wichtig, sondern auch in regionalen und überregionalen Zusammenhängen:

- *Regionale Kooperation* (wie sie bei den *MEDIA*@Komm-Projekten besonders im Städteverbund Nürnberg und bei Esslingen mit der Einbindung in die Wirtschaftsförderungsregion Stuttgart angelegt ist);
- *Städtekooperation* zum Austausch von Erfahrungen und guten Lösungen, zur Bildung von Entwicklungspartnerschaften unter Hilfestellung der kommunalen Spitzenverbände und anderer kommunaler Organisationen; ein Beispiel dafür ist der Arbeitskreis Digitale Signatur/Chipkarten (AK DSC) des Deutschen Städtetages (DST);
- Verknüpfung lokaler/regionaler Netze mit überregionalen, internationalen und globalen Netzen (Informationsnetze, persönliche Netze, wirtschaftliche Netze).

Dabei ist offensichtlich, dass auch die Städte und die Projekte in Konkurrenz zueinander stehen. Mehr denn je befinden sich Gebietskörperschaften „unter dem Primat der Ökonomie“ im Wettbewerb um gute Lösungen, um sich als leistungsfähige und lebenswerte Unternehmens- und Wohnstandorte zu profilieren[128]. Dies schließt Kooperation und Abstimmung aber nicht aus, sondern erzwingt sie geradezu. Keine Stadt hat in der Regel für sich allein die Kraft und Innovationsfähigkeit, entsprechende gute Querschnittslösungen, wie sie für MEDIA@Komm typisch sind, zu entwickeln und möglicherweise sogar allgemeine Standards zu setzen. Notwendig ist eine thematisch und zeitlich definierte und möglicherweise auch begrenzte Zusammenarbeit. In den USA wurde für diesen erfolgsträchtigen Weg der Konkurrenz bei gleichzeitiger Kooperation der Begriff „coopetition“ (competition und co-operation) gewählt[129]. Nach einer

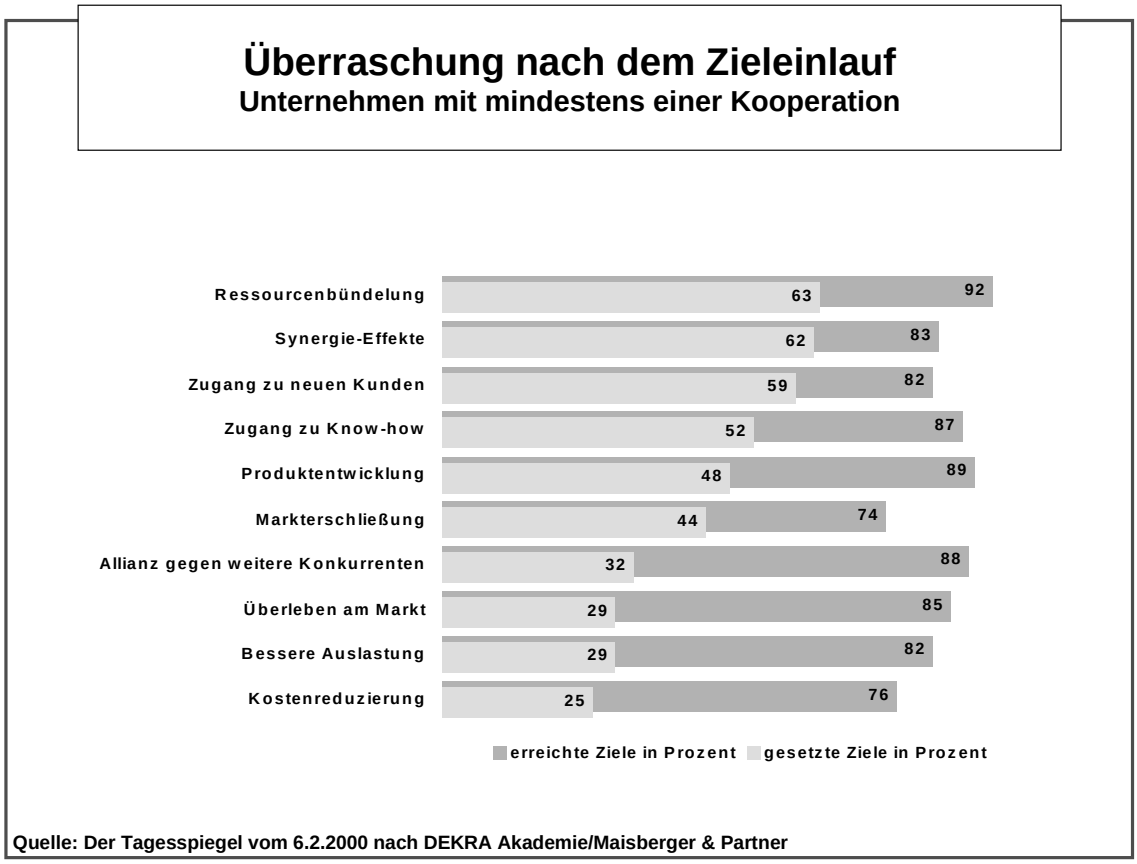
127 Vgl. z.B. *Axel Zerdick u.a.*, Die Internet-Ökonomie. Strategien für die digitale Wirtschaft, Berlin u.a. 1999, S. 151 (European Communication Council Report).

128 Vgl. z.B. *Heinrich Mäding (Hrsg.),* Zwischen Überforderung und Selbstbehauptung – Städte unter dem Primat der Ökonomie, Berlin 1999 (Difu-Beiträge zur Stadtforschung, Bd. 28).

129 Vgl. z.B. *Dietrich Henckel*, Kommunen und Kooperation, in: Dietrich Henckel, Holger Floeting, Busso Grabow u.a., Entscheidungsfelder städtischer Zukunft, Stuttgart u.a. 1997, S. 297-329 oder *Werner*

jüngst veröffentlichten Studie in Deutschland kooperieren inzwischen sechs von zehn Unternehmen mit ihren Mitbewerbern[130]. Die Ziele der Kooperation lassen sich in vielerlei Hinsicht auch auf Kommunen übertragen (vgl. Abbildung)

Abbildung: Ziele bei Unternehmenskooperationen unter Wettbewerbern



Kooperationen sind auch deshalb wichtig, weil sie den Wert der „Netze“ steigern. Der Wert von Netzwerken (beispielsweise des Netzwerks der mit der digitalen Signatur durchzuführenden Dienstleistungen) steigt mit der Koordinierung kleinerer Netze[131] (wie etwa von Netzen der an Baugenehmigungsverfahren Beteiligten – Kommunen, Private, Intermediäre – oder die Kooperation der Anbieter verschiedener Produkte und Dienstleistungen rund um den elektronischen Geschäftsverkehr). Auch die Schaffung gemeinsamer Plattformen für öffentliche Online-Services und E-Commerce (vgl. unten) ist ein wichtiger Schritt zur Vergrößerung und damit zur Wertsteigerung von Netzwerken.

Heinz (Hrsg.), Stadt & Region – Kooperation oder Koordination? Ein internationaler Vergleich, Berlin 2000 (Schriften des Deutschen Instituts für Urbanistik, Bd. 93).

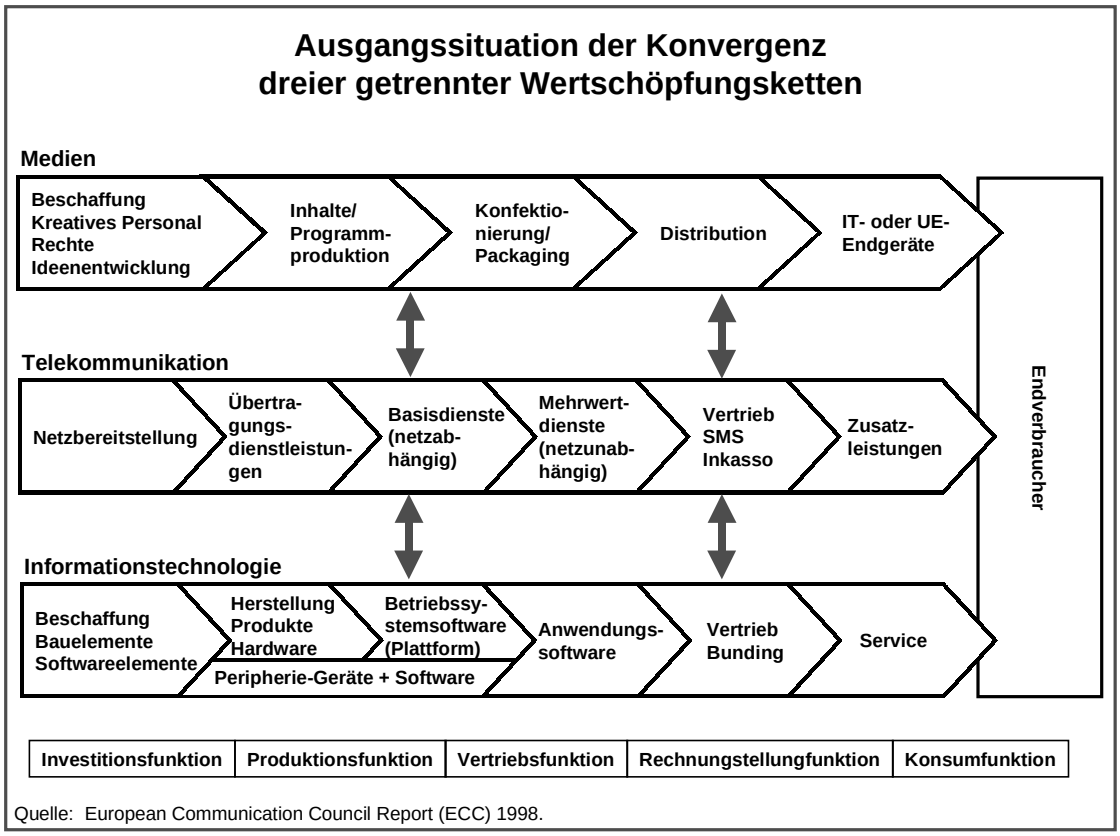
130 „Gemeinsame Sache mit dem Wettbewerber“, Tagesspiegel vom 6.2.2000.

131 Vgl. z.B. *Kevin Kelly*, NetEconomy, München und Düsseldorf 1998, S. 56.

4.3 Gemeinsame Plattformen für öffentliche Online-Services und E-Commerce

Auf die Konvergenz der Sektoren Medien, Kommunikation und Informationsverarbeitung wurde bereits hingewiesen[132]. Diese Konvergenz führt auch dazu, dass Information, Kommunikation, Transaktion aus Sicht der Anbieter und der Nutzer zusammenwachsen; deutlich wird dies beispielsweise bei den fortgeschrittenen Stadtinformationssystemen[133]. Schließlich ist auch die Konvergenz von Endgeräten, der Sicherheits- oder Transaktionsinfrastruktur zu beobachten, unabhängig davon, wer der Anbieter der Informationen, Produkte oder Dienstleistungen ist.

Abbildung: Konvergenz ehemals getrennter Wertschöpfungsketten*



Quelle: European Communication Council Report (ECC) 1998.

* Quelle: Nach *Axel Zerdick u.a.*, Die Internet-Ökonomie. Strategien für die digitale Wirtschaft (European Communication Council Report), Berlin u.a. 1999, S. 129 ff.

Allein schon wegen dieser Konvergenz ist es auch sinnvoll, gemeinsame Plattformen für öffentliche Online-Services und E-Commerce zu nutzen. Die meisten Komponenten elektronischen Geschäftsverkehrs sind gleichermaßen für Kommunikations- und Transaktionsprozesse zwischen Öffentlichen und Privaten nutzbar. Verknüpfen und als

132 Vgl. unter anderem *Axel Zerdick u.a.*, Die Internet-Ökonomie. Strategien für die digitale Wirtschaft, Berlin u.a., 1999, S. 129 ff. (European Communication Council Report).

133 Vgl. *Steffi Bütow und Holger Floeting,* Elektronische Stadt- und Wirtschaftsinformationssysteme in deutschen Städten, Stuttgart 1999.

Komplettangebote bereitstellen (wie dies im Bremer MEDIA@Komm-Konzept teilweise geschehen soll) lassen sich:

- Infrastruktureinrichtungen, wie z.B. www-Server, Server für Sicherheitsdienstleistungen, Server für den elektronischen Zahlungsverkehr, Datenbankserver, Formularserver (die teilweise physisch integriert, teilweise physisch getrennt sind), Trust Center, Netzinfrastrukturen, Kioske,
- entsprechende Software zur Nutzung der Infrastruktur,
- Dienstleistungen zur direkten Abwicklung der Angebote und als Zusatzservices.

Information, Kommunikation und Transaktion sowie Sicherheit wachsen dabei genauso zusammen wie die verschiedenen Zugangs- und Nutzungswege elektronischen Geschäftsverkehrs.

5. Stand der Normung zur IT-Sicherheit, digitalen Signatur und bei Identifikationskarten [Autor: Arnold Schulz (DIN)]

Normen und Standards schaffen Voraussetzungen für freien und fairen Handel sowie den Austausch von Informationen. Sie fördern damit den Wettbewerb, unterstützen somit wirtschaftliches Wachstum und schützen den Verbraucher und Anwender. Auch im Dienstleistungsbereich wird die Bedeutung von Standards zunehmend erkannt, insbesondere seit der Erweiterung des General Agreement on Tariffs and Trade (GATT) auf Dienstleistungen. Die Welthandelsorganisation (WTO) und die Internationale Organisation für Normung (ISO) haben daher Initiativen gestartet, internationale Standards und Normen im Dienstleistungssektor zu entwickeln und anzuwenden.

Das DIN Deutsches Institut für Normung e.V. ist ein technisch-wissenschaftlicher Verein und das für die Normungsarbeit in der Bundesrepublik Deutschland zuständige Institut sowie durch einen Staatsvertrag („Normenvertrag“) auch der alleinige Zuständige in Deutschland für die europäische und internationale Normung. Zur Realisierung der Normungsarbeit in innovativen Projekten hat das DIN das Instrument *der Entwicklungsbegleitenden Normung* geschaffen. Ziel ist es, nicht mehr nur die Fortschritte der technischen Entwicklung festzuhalten und in technischen Regeln zu definieren, sondern integraler Bestandteil der technischen Neuerungen und der damit verbundenen Forschung und Entwicklung (F&E) zu werden und somit den Wissens- und Technologietransfer zu fördern und zu beschleunigen. Dazu gibt es neben der Möglichkeit der „klassischen“ Normung neue, schnellere Verfahren, wie die Veröffentlichung von Diskussionsergebnissen zur Normung in DIN-Fachberichten oder die Herausgabe öffentlich verfügbarer Spezifikationen (PAS). Diese neuen Möglichkeiten sollen im Projekt *MEDIA*@Komm vor allem genutzt werden, um frühzeitig zu allgemein anerkannten Vereinbarungen zu kommen. Damit sollen die Transparenz und Effektivität der erarbeiteten Lösungen unterstützt und deren Anwendung nach einheitlichen Kriterien gesichert werden.

Für die klassische Normung auf dem Gebiet der IT-Sicherheit und Digitalen Signatur ist im DIN Deutsches Institut für Normung e.V. der Normenausschuss Informationstechnik (NI) zuständig. Unter den zehn Arbeitsgebieten des NI werten die interessierten Kreise die IT-Sicherheit als wichtigstes Arbeitsgebiet. Der NI führt neben den nationalen Gremien für IT-Sicherheitsverfahren (NI-27) und Identifikationskarten (NI-17) das Sekretariat des internationalen Normungsgremiums für die IT-Sicherheit, ISO/IEC JTC 1/SC 27 „Security“ sowie das Sekretariat des europäischen Workshops für die elektronische Signatur, CEN/ISSS WS/E-Sign (www.cenorm.be/isss/Workshop).

Die auf dem Gebiet der IT-Sicherheit in Deutschland tätigen Normungsgremien konzentrieren sich auf die aktive Mitwirkung an der Entwicklung Internationaler Normen und deren direkte Anwendung in der Originalsprache.

Im Mai 1999 führte der NI einen DIN-Workshop zur „Branchenübergreifenden digitalen Identität“ durch, als dessen Ergebnis unter anderem die Arbeitsgruppe „Interoperabilität digitaler Identität“ gebildet wurde. Die Aufgabe dieser Arbeitsgruppe besteht in der Abstimmung der deutschen Position zu Fragen der elektronischen Signatur und digitalen Identität und deren wirksamer Vertretung in der europäischen und internationalen Normung.

Ausgangspunkt war eine Empfehlung der Kommission Informationsgesellschaft (KIG) im DIN, dass das DIN eine Plattform organisieren sollte, mit deren Hilfe die vielfältigen Aktivitäten zur Normung und Spezifikationsentwicklung auf diesem Gebiet gebündelt werden können.

In Vorbereitung dieses Workshops wurde die Situation im Normungsbereich gründlich analysiert. Sie lässt sich folgendermaßen zusammenfassen:

- Die Komplexität der Anwendungen im IT-Bereich verlangt, dass rechtliche, soziale, fiskalische und technische Regelungen zusammenwirken und sich ergänzen müssen.
- Grundlegende Normen sind meist vorhanden, die in verschiedenen Normenausschüssen erarbeitet wurden. Ihre anwendungsbezogene Kombination ist oft schwierig, es gibt dafür auch keine übergeordneten Gremien.
- Es gibt im Kommunikationsbereich eine Vielzahl oft konkurrierender Aktivitäten von Unternehmen oder Konsortien, die nicht zielgerichtet koordiniert werden.
- Im Bereich der Normung zeigen Unternehmen und Einrichtungen eher eine abwartende Haltung, oft fehlt die Bereitschaft, eigene Ressourcen dafür einzusetzen.

Ähnliche Ergebnisse brachten auch Untersuchungen zur technischen Umsetzung des Signaturgesetzes, die von der KIG durchgeführt wurden. Die KIG wurde 1995 gebildet, um ausschussübergreifend die Anforderungen an die Normung im Bereich der Informations- und Kommunikationstechnik zu analysieren und einer Lösung zuzuführen.

Spätestens seit der starken, weltweiten Verbreitung des Internets müssen neue Normen, Spezifikationen, Richtlinien und andere Vereinbarungen auf internationaler Ebene definiert und akzeptiert werden. Als problematisch haben sich bei den Standardisierungsbestrebungen die sehr unterschiedlichen nationalen Auffassungen von Datenschutz und Privatsphäre erwiesen. Um bei diesen unterschiedlichen Auffassungen überhaupt ein Ergebnis zu erzielen, muss häufig ein Konsens auf sehr niedriger Ebene gesucht werden. Bislang bieten die Internationale Organisation für Normung (ISO) und die Internationale Elektrotechnische Kommission (IEC) die beste Plattform für die Vereinheitlichung von Rahmenbedingungen, wenn auch von vielen Akteuren in diesem Bereich auf die recht lange Zeitdauer dieser Arbeiten kritisch hingewiesen wird. Die besondere Eignung von ISO und IEC liegt wohl vor allem daran, dass gerade bei mehrseitiger Sicherheit und Datenschutz die Beteiligung möglichst vieler interessierter Kreise wichtig ist.

Das DIN richtet gegenwärtig seine Anstrengungen darauf, die Vielzahl der auf diesem Gebiet tätigen Einrichtungen mit ihren speziellen Arbeitsverfahren und Produkten koordiniert einzubeziehen. Dies betrifft vor allem die Entwicklung von Normen bzw. öffentlich verfügbaren Spezifikationen (PAS) im DIN, vertiefende DIN-Workshops über die künftige Strategie sowie die Entwicklung von Spezifikationen in Organisationen außerhalb des DIN.

Verstärkt sollen in diese Aktivitäten auch Regierungseinrichtungen und Behörden einbezogen werden. Ihre Funktion besteht in diesem Zusammenhang weniger in der Beaufsichtigung und Regulierung als vielmehr in der Rolle eines kompetenten Marktteilnehmers mit allen daraus resultierenden Rechten und Pflichten.

Die Einbringung der deutschen Position in die europäische und internationale Normungsarbeit verlangt, dass mehr Akteure und vor allem die Marktführer sich stärker im Normungsprozess engagieren.

5.1 Normen für die IT-Sicherheit

Die vorhandenen Normen und Fachberichte zur IT-Sicherheit betreffen insbesondere

- grundlegende Definitionen, Vorgehensweisen und Modelle,
- IT-Sicherheitsmechanismen einschließlich Schlüsselverwaltung sowie
- Kriterien und Verfahren für die Evaluation von IT-Sicherheit.

Sie beziehen sich vielfach auf Festlegungen in Normen anderer Gebiete, insbesondere der Informationstechnik. Die wichtigsten Normen sind nachfolgend genannt.

Die Normung von IT-Sicherheit stützt sich auf den allgemeinen Begriff von Sicherheit in der Technik nach

DIN VDE 31000-2
Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse; Begriffe der Sicherungstechnik; Grundbegriffe

Als Vorstufe der Normung wurden erste Richtlinien zur Gewährleistung von IT-Sicherheit in den folgenden Fachberichten der ISO und IEC veröffentlicht.

ISO/IEC TR 13335 Informationstechnik; Richtlinien für das Management von IT-Sicherheit Guidelines for the management of IT security (GMITS)

Teil 1: Konzepte und Modelle für die IT-Sicherheit (DIN-Fachbericht 66)
Teil 2: Management und Planung von IT-Sicherheit
Teil 3: Techniken für das Management von IT-Sicherheit
Teil 4: Auswahl von Schutzmechanismen
Teil 5: Schutzmechanismen für externe Verbindungen

Das Management von IT-Sicherheit wird als Prozess aufgefasst, der dazu dient, die geforderten Niveaus von Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit (Verbindlichkeit) und Authentizität von Daten, Systemen und Diensten herzustellen und aufrechtzuerhalten. Ausgangspunkt sind

- die zu schützenden (Informations-)Werte,
- die abzuwehrenden Gefahren bzw. Bedrohungen,
- die Sicherheitsziele

der jeweiligen Organisation. Unter Berücksichtigung definierter Sicherheitsanforderungen und möglicher Einschränkungen finanzieller, rechtlicher oder sozialer Natur sind die erforderlichen Schutzmaßnahmen festzulegen. Ihre Implementierung ist zu beaufsichtigen. Die getroffenen Maßnahmen sind kontinuierlich unter Zugrundelegung der aktuellen Werte, Bedrohungen und Sicherheitsziele zu überprüfen und gegebenenfalls zu verändern (siehe Bild 1).

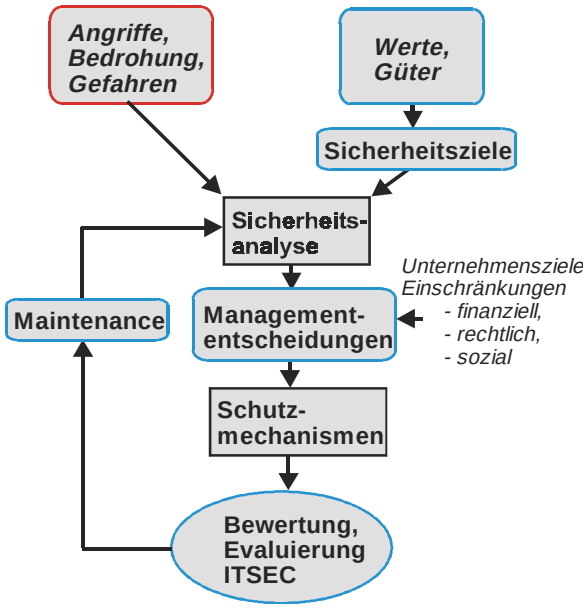


Bild 1: Management von IT-Sicherheit

Zur Sicherung der Interoperabilität wurden mit der Norm

> ISO/IEC 9979 Informationstechnik; Sicherheitsverfahren; Verfahren für die Registrierung von kryptographischen Algorithmen

Verfahren bereitgestellt.

Die Norm beschreibt Verfahren für das Registrieren eines Algorithmus, die Form der Registereintragungen, die Aufgaben der Registraturbehörde und die Verantwortung des Antragstellers.

Es sind aktuell 20 kryptische Algorithmen registriert:

- Für Einwegverfahren ohne Schlüssel, Hash-Funktionen

Festlegungen zur Anwendung von Hash-Funktionen für die eindeutige Identifikation von Nachrichten treffen die Normen

ISO/IEC 10118 Informationstechnik; Sicherheitstechniken; Hash-Funktionen;

Teil 1: Allgemeines Modell
Teil 2: Hash-Funktionen unter Benutzung eines n-bit-Blockschlüssel-Algorithmus
Teil 3: Zugeordnete (dedizierte Hash-Funktion)
Teil 4: Hash-Funktion unter Benutzung modularer Arithmetik

- Verfahren mit symmetrischem Schlüssel (kaum Bedeutung für *MEDIA*@Komm)

In den folgenden Normen werden vier Verfahren beschrieben.

ISO 8372 Informationsverarbeitung; Betriebsarten für einen 64-bit-Blockschlüssel-Algorithmus

ISO/IEC 10116 Informationstechnik; Sicherheitsverfahren; Betriebsarten für einen n-bit-Blockschlüssel-Algorithmus

- Verfahren mit asymmetrischem Schlüssel und digitale Signatur

Das deutsche Signaturgesetz sieht die digitale Signatur mit Hilfe der asymmetrischen Verschlüsselung vor. Für diese Verfahren liegen bereits mehrere internationale Normen vor, die auch in Deutschland zur Anwendung kommen.

ISO/IEC 9796 Informationstechnik; Sicherheitsverfahren; Digitales Unterschriftsverfahren mit Rückgewinnung der Nachricht

ISO/IEC 14888 Informationstechnik; Sicherheitsverfahren; Digitale Unterschrift mit Anhang

ISO/IEC CD 15946 Informationstechnik – Sicherheitsverfahren – Kryptographische Techniken auf der Grundlage elliptischer Kurven

ISO/IEC 9797 Informationstechnik; Sicherheitsverfahren – Mechanismus zur Sicherung der Datenintegrität mit Hilfe kryptographischer Funktionen Nachrichten-Authentifizierung-Codes (MACs)

ISO/IEC 9798 Informationstechnik; Sicherheitstechniken; Mechanismen zur Authentifizierung von Instanzen

ISO/IEC 13888 Informationstechnik; Sicherheitstechniken; Nicht-Abstreitbarkeit (non-repudation)

- Normen für das Schlüssel-Management

Diese Normen beschreiben Verfahren für die Generierung und Bereitstellung (Transport) von Schlüsseln sowie Verantwortung und Dienste vertrauensgenießender Einrichtungen.

Für die Handhabung von Schlüsselmaterial zur Anwendung in Verschlüsselungssystemen sind in

ISO/IEC 11770 Informationstechnik; Sicherheitsverfahren; Schlüssel-Management

Festlegungen enthalten.

Im Technischen Bericht

ISO/IEC DTR 14516 Informationstechnik; Sicherheitsverfahren; Richtlinien für die Verwaltung und Nutzung von Diensten vertrauensgenießender dritter Seiten (trusted third parties, TTP)

werden Aufgaben, Verantwortungen und Beziehungen zu TTP-Einrichtungen und Nutzern ihrer Dienste behandelt.

Ein Normungsvorhaben in der ISO/IEC soll speziell diejenigen Dienste für TTPs spezifizieren, die digitale Signaturen unterstützen und dabei die Interoperabilität sichern. Dazu liegt ein Entwurf vor.

ISO/IEC CD 15945 Informationstechnik; Sicherheitsverfahren; Spezifikationen der TTP-Dienste zur Unterstützung der Anwendung der digitalen Signatur

- Normen für die Evaluierung der Sicherheit von IT-Systemen

ISO/IEC 15408 Informationstechnik; Sicherheitsverfahren; Evaluationskriterien für IT-Sicherheit

legt die Vorgehensweise bei der Evaluierung und die Evaluationskriterien fest.

Der Herstellung und Registrierung von Schutzprofilen dienen die Normen

ISO/IEC 15446 Informationstechnik; Sicherheitsverfahren; Richtlinien für die Herstellung von Schutzprofilen

ISO/IEC 15292 Informationstechnik; Sicherheitsverfahren; Verfahren für die Registrierung von Schutzprofilen

5.2 Normen für Identifikationskarten

Für kontaktorientierte Chipkarten ist die zehnteilige Normenreihe ISO/IEC 7816 die grundlegende internationale Norm. Während die Teile 1 und 2 die physikalischen Eigenschaften der Karten festlegen, beschreiben die anderen acht Teile die Austauschprotokolle, die zwischen Chipkarte und Kartenleser zum Einsatz kommen.

Vor allem im Transportbereich finden seit 1994 kontaktlose Chipkarten Anwendung. Drei verschiedene Typen von kontaktlosen Chipkarten vom Typ ID-1 gemäß ISO/IEC 7810 werden zurzeit in jeweils vierteiligen Normenreihen genormt, wobei die Normung bei allen drei Typen im Wesentlichen kurz vor ihrem Abschluss steht. Dabei beschreibt die Normenreihe ISO/IEC 10536 die Parameter von Chipkarten, die für den Einsatz in sehr geringem Abstand (0 bis 2 mm) vom Kartenlesegerät bestimmt sind („Close-coupled“-Karten), die Reihe ISO/IEC 14443 Karten für etwas größere Abstände, 0 bis 10 cm („Proximity“-Karten) und die Reihe ISO/IEC 15693 Karten für Abstände bis zu einem Meter („Vicinity“-Karten).

Zu den Normen für Identifikationskarten mit Magnetstreifen und/oder aufgeprägten Schriftzeichen gehören vor allem die Normen der Reihe ISO/IEC 7811, die die physi-

kalischen Charakteristika der Karten beschreiben. ISO/IEC 7811 befindet sich zurzeit in Überarbeitung. Sie beschreibt diverse Aufzeichnungstechniken.

Registrierung und Management der Registrierungen werden durch die Reihe ISO/IEC 7812 genormt. ISO/IEC 7812 beschreibt insbesondere ein Nummerierungssystem für die Identifizierung von Kartenherausgebern sowie das dazugehörige Antrags- und Registrierungsverfahren.

Für die speziellen Zwecke der Telekommunikation gibt es eine Reihe von europäischen Normen für Chipkarten, die in das deutsche Normenwerk übernommen worden sind. Diese Normen wurden vom CEN-Komitee TC 224, „Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren“, erarbeitet. Sie liegen im Allgemeinen in deutscher Sprache vor.

Auf Wunsch des Banksektors wurde vom CEN-Komitee TC 224, „Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren“, eine dreiteilige Vornormenreihe erarbeitet, die in das Deutsche (Vor-)Normenwerk übernommen worden ist. Die Reihe umfasst Kartensysteme mit Magnetspur, Karten mit integriertem Schaltkreis und gemischte Systeme, die in den Vornormen DIN V ENV 1257-1, DIN V ENV 1257-2 und DIN V ENV 1257-3 enthalten sind.

Die gleichfalls vom CEN-Komitee TC 224, „Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren“, erarbeitete Reihe der europäischen Normen EN 1332 legt im Rahmen der Beschreibung der Mensch-Maschine-Schnittstelle die Gestaltungsgrundsätze für die Anwenderschnittstelle, die taktilen Kennzeichen, die bei der Gestaltung von maschinenlesbaren Karten zu berücksichtigen sind, und die Standardanordnung für Blocktastaturen von kartenbetriebenen Geräten fest. Diese Festlegungen sind branchenübergreifend.

Für das Gesundheitswesen sind die beiden DIN-Normen DIN EN 1387:1997 und DIN EN 1867:1997 gültig, die aus europäischen Normen durch Übernahme hervorgegangen sind.

Für den landgebundenen Personenverkehr und Gütertransport beschreibt DIN V ENV 1545-1 die Datenelemente für Applikationen auf maschinenlesbaren Karten, während Teil 2 diese Datenelemente in Datenstrukturen ordnet, die bei verschiedenen Applikationen des landgebundenen Verkehrs angewendet werden können.

Für die elektronische Geldbörse definiert DIN EN 1546 Teil 1 bis Teil 4 Schnittstellen und die Funktionalität für IEP-Systeme (Systeme der brachenübergreifenden elektronischen Geldbörse).

Für die Beschreibung der Schnittstelle zur Chipkarte (IFD/ICC-Schnittstelle) für Chipkarten mit Digitaler Signatur-Anwendung wird gegenwärtig eine DIN-Vornorm erarbeitet. Die DIN V 66291-1 „Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV“ liegt als Entwurf vor und wird in diesem Jahr veröffentlicht.

5.3 Normen für den elektronischen Geschäftsverkehr

Im September 1999 wurde der Norm-Entwurf DIN 16557-4 „Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Regeln zur Auszeichnung von UN/EDIFACT-Übertragungsstrukturen mit der Extensible Markup Language (XML) unter Einsatz von Document Type Definitions (DTDs)“ veröffentlicht.

Gleichzeitig stellte Deutschland den Antrag für ein internationales Normungsvorhaben im zuständigen Komitee der ISO. Bis Ende März 2000 haben die Mitgliedsländer von ISO/TC 154 die Möglichkeit, über diesen Antrag abzustimmen und gleichzeitig Kommentare zum deutschen Vorschlag zu geben.

In Verbindung mit EDI wird XML als ein relativ einfacher und kostengünstiger Einstieg für kleine und mittelständische Unternehmen in den durchgängigen elektronischen Datenaustausch eines Geschäftsvorfalls gesehen, z.B. Anfrage einholen – Angebot empfangen – Bestellung absenden – Liefermeldung senden – Rechnung stellen – Zahlung an die Bank – Belastungs- und Gutschriftanzeige von der Bank empfangen.

5.4 CEN – Workshop – Agreements (CWA)

Innerhalb der europäischen Normungsorganisation CEN wurde seit 1997 ein neues Verfahren entwickelt, um in kürzeren Zeiträumen Vereinbarungen auszuarbeiten und als CWA zu veröffentlichen. Vor allem im Bereich der Informations- und Kommunikationstechnologie wird diese Möglichkeit in zunehmenden Maße genutzt. CWA haben einen ähnlichen Charakter wie die im nationalen Rahmen herausgegebenen öffentlich verfügbaren Spezifikationen (PAS).

CWA werden im Rahmen von Konsortien entwickelt. Sie unterscheiden sich von Europäischen Normen dadurch, dass sie grundsätzlich kein öffentliches Einspruchsverfahren durchlaufen und dass auch keine nationale Meinungsbildung stattfindet, d.h., CWA haben lediglich die Zustimmung der unmittelbar beteiligten Mitglieder des Konsortiums gefunden.

CWA werden ausschließlich in englischer Sprache herausgegeben und sollten möglichst die Basis für die spätere Erarbeitung von Normen sein.

Im Zusammenhang mit den bei *MEDIA*@Komm vorgesehenen Entwicklungen sind die folgenden CWA von Bedeutung.

CWA 13404 Katalog übergeordneter Benennungssysteme und Inkompatibilitätsfragen in der Informationstechnik

CWA 13449 1 bis 12 Erweiterungen für die Schnittstellenspezifikation für Finanzdienstleistungen

CWA 13679 Richtlinien für Benennungen in einer Internet-Umgebung

CWA 13692 Harmonisierung von Produktions- und Geschäftsdaten (PBDH)

CWA 13699 Anforderungen für Metadata für Multimediainformation

CWA 13700 Modell für Metadata für Multimediainformation

Weitere CWA sind gegenwärtig noch in der Phase der Erarbeitung. Für das Projekt wichtige Themen sind:

Electronic Commerce

- Electronic Signatures
- Metadata for Multimedia-Information
- Quality of Internet Services

Nähere Informationen zum aktuellen Bearbeitungsstand der CWA werden auf der www-Seite von CEN (www.cenorm.be/isss/Workshop) veröffentlicht.