Via Internet zum papierlosen Büro? Ein Pilotprojekt zur sicheren Informationsübermittlung in der hessischen Landesverwaltung

Von Andreas Hedwig

Seit einigen Jahren geistert das Menetekel vom *papierlosen Büro* durch die Zukunftsdiskussionen der Archivare. Wie es aussehen wird, zeichnet sich immer deutlicher ab,[1] und klar ist: Wenn es eines Tages soweit ist und die Behörden ihren Geschäftsgang vollständig auf elektronische Datenverarbeitung umstellen, dann müssen die Archive in der Lage sein, elektronische Dokumente auf Dauer zu sichern. Andernfalls können sie ihre Aufgaben nicht mehr erfüllen. Mit gleichförmigen, strukturierten Massendaten sehen sie sich schon heute konfrontiert, und einige schaffen inzwischen Vorkehrungen für den Tag X, da diese tatsächlich archiviert werden müssen.[2]

Wie weit sind die IT-Anwendungen aber im Bereich der Bürokommunikation in der Praxis vorangeschritten, gibt es inzwischen eine greifbare Perspektive für den papierlosen Geschäftsgang? Interessante, vielleicht typische Entwicklungen sind in der hessischen Landesverwaltung zu beobachten. Zur Zeit wird dort ein Pilotprojekt mit dem Titel *Ende-zu-Ende Verschlüsselung für den elektronischen Datenaustausch* durchgeführt. Es werden also Verfahren getestet, welche zweifellos in absehbarer Zeit starken Einfluß auf die Bürokommunikation haben werden.

Die im folgenden angesprochenen Dienststellen sind komplex arbeitende oberste und obere Landesbehörden, deren typisches Schriftgut die differenzierte Sachakte mit – aus archivischem Blickwinkel – hohem Quellenwert ist. Es erhebt sich die Frage, wie weit wird die Büroautomation auch dieses zentrale Schriftgut erfassen? Droht auch der differenzierten Sachakte bald die digitale Zukunft?

Das Projekt wurde zunächst im Unterausschuß Büroautomation (UABA) des Landes-Automationsausschusses (LAA) vorgestellt. Dieser existiert seit 1986 und

---

[1] Vgl. etwa die bei Michael *Wettengel:* Digitale Signaturen und Pilotprojekte zur IT-gestützten Vorgangsbearbeitung in der Bundesverwaltung. In: Frank M. *Bischoff* (Hg.): Archivierung von Unterlagen aus digitalen Systemen. Beiträge zur Tagung im Staatsarchiv Münster. 3.–4. März 1997 (Veröffentlichungen der staatlichen Archive des Landes Nordrhein-Westfalen E 4). Münster 1997. S. 13–18, beschriebenen Projekte sowie den Handlungsleitfaden IT-gestützte Vorgangsbearbeitung. Hg. vom Bundesministerium des Innern (Schriftenreihe der KBSt 35). Bonn 1997. – Vgl. zur Anwendungsseite letzteren sowie DOMEA. Aufbau eines Pilotsystems für Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang. Hg. v. Bundesministerium des Innern (Schriftenreihe der KBSt 34). Bonn 1997.

[2] Vgl. Gudrun *Fiedler:* Archivierung von Unterlagen aus digitalen Systemen am Beispiel des Landes Niedersachsen. In: Frank M. *Bischoff* (Hg): Archivierung von Unterlagen aus digitalen Systemen. Beiträge zur Tagung im Staatsarchiv Münster. 3.–4. März 1997 (Veröffentlichungen der staatlichen Archive des Landes Nordrhein-Westfalen E 4). Münster 1997. S. 21–29.

wird federführend vom Hessischen Ministerium des Inneren geleitet. Ihm gehören insbesondere die EDV-Referenten der zentralen Landesbehörden, der Hessische Datenschutzbeauftragte sowie die Hessische Zentrale für Datenverarbeitung an. Seit Ende 1992 ist das Hauptstaatsarchiv Wiesbaden dort vertreten.

Der UABA sieht seine Aufgabe vornehmlich darin, in die Entwicklungen der Büroautomationstechniken und deren Anwendungen innerhalb der hessichen Landesverwaltung regelnd einzuwirken. Dies tut er mittels Empfehlungen – etwa zu Kriterien des Datenschutzes und der Datensicherheit oder zu Systemstandards. Im Falle der automatisierten Schriftgutverwaltung bündelte der UABA beispielsweise Spezialwissen und hatte so entscheidenden Anteil daran, daß Insellösungen weitgehend verhindert werden konnten.

Andererseits fungiert der Ausschuß als Informationsbörse: In mehr oder weniger regelmäßigen Abständen referieren die Mitglieder über den Stand der Büroautomation in ihren Behörden; hinzu kommen Berichte und Diskussionen um Punkte oder Initiativen, die von außen an den Ausschuß herangetragen wurden, zum Beispiel durch den Kooperationsausschuß ADV Bund/Länder/Kommunaler Bereich (KoopA ADV), das Bundesamt für Sicherheit in der Informationstechnik (BSI), oder solche, die sich durch neue technische Entwicklungen ergeben.

Der bereits genannte Projektantrag, der vom UABA in den solche Angelegenheiten entscheidenden LAA übermittelt wurde, betrifft den Bereich Verschlüsselung von Informationen und digitale Signatur bei der Übertragung von Informationen über das Internet. In einem Arbeitspapier mit dem Titel *Verschlüsselung und elektronische Signatur in der öffentlichen Verwaltung Hessens* vom Juli 1997[3] befaßte sich die HZD mit folgenden Punkten:

- Sie stellte die derzeit auf dem Markt gehandelten Verschlüsselungsverfahren vor[4] und diskutierte deren Qualität und den zu erwartenden Kostenaufwand für die Beschaffung;
- weiter entwickelte sie in groben Zügen, wie sich nach den Erfordernissen des zu dem Zeitpunkt kurz vor der Veröffentlichung stehenden Informations- und Kommunikationsdienste-Gesetzes (IuKDG)[5] der Aufbau einer Sicherheitsstruktur in der hessischen Landesverwaltung gestalten müßte;
- und schließlich widmete sie sich der Frage, wie erste Schritte in diese Richtung unternommen werden könnten.

Der letzte Punkt mündete in einen Antrag mit dem Titel: *Ende-zu-Ende Verschlüsselung für den elektronischen Datenaustausch. Pilotprojekt zum Aufbau einer IT-Sicherheitsinfrastruktur.*[6]

Die Motive für diesen Antrag lagen keineswegs nur in den Vorgaben des IuKDG. Den konkreten Hintergrund gab die bislang geübte Praxis im Bereich der elektronischen Datenübermittlung ab. Dieses Thema beschäftigt den UABA seit 1994. Gemäß der Vereinbarung zwischen Bund und Ländern wurde in Hessen zu-

[3] Vorlage für die UABA-Sitzung vom 18. Juli 1997.

[4] Vgl. hierzu Michael *Wettengel*: Digitale Unterschriften. In: Der Archivar 50 (1997) Sp. 90–94.

[5] Bundesgesetzblatt 1997. Teil I. S. 1870. – Vgl. zur Entstehung Michael *Wettengel*, wie Anm. 1, S. 11–13.

[6] Vorlage für die UABA-Sitzung vom 9. September 1997.

nächst in der HZD eine X.400-Kopfstelle eingerichtet und nach und nach ein landesweites Kommunikationsnetz ausgebaut. Der Mail-Standard X.400 galt zu diesem Zeitpunkt, als vom Internet unabhängiges, die Teledienste nutzendes Datenübertragungssystem, insbesondere aus Sicherheitsaspekten für den behördlichen Gebrauch als besonders geeignet.[7] Eine Alternative war zunächst nicht in Sicht.

Parallel entwickelte sich jedoch in stürmischer Weise das Internet, das konkurrenzlos dastand für den raschen Zugriff auf aktuelle Informationen. Selbstverständlich ging auch die hessische Landesregierung aktiv auf das Internet zu und erarbeitete zum Beispiel eine Präsentation der Landesverwaltung mit eigenen Informationsdiensten.[8] In den letzten zwei Jahren traten jedoch die dort vorhandenen Möglichkeiten der e-mail, nun auch in verschlüsselter Form, in den beteiligten Behörden X.400 als kostengünstige Alternative im Bereich des Dokumentenaustausches gegenüber. Die Anwender erhoffen sich durch die kostengünstige Nutzung des Internets insbesondere, die bisher vergleichsweise hohen Produktiv-, Übertragungs- sowie Administrationskosten einsparen zu können.[9]

Selbstverständlich geht es der HZD bei der Durchführung des Projekts zunächst um die Bewältigung der technischen Probleme, d. h. die *Interoperabilität zwischen verschiedenen Systemplattformen zu untersuchen [...] Das Pilotprojekt soll zeigen, wie sich beim elektronischen Datenaustausch eine zuverlässige Ende-zu-Ende Datenverschlüsselung einerseits und eine eindeutige Authentisierung mittels Digitaler Signatur andererseits in die vorhandene PC-Ausstattung der Dienststellen der hessischen Landesverwaltung integrieren läßt. Weiterhin soll untersucht werden, in welcher Form Verschlüsselung und Digitale Signatur zum Schutz von Daten auf lokalen Systemen einsetzbar sind.* Eine Testgemeinde ist inzwischen mit entsprechender Software ausgestattet. Die HZD soll ihrerseits die Voraussetzungen schaffen, um als TrustCenter für die Testgemeinde zu fungieren; sie übernimmt die Rolle der Zertifizierungsinstanz und die Aufgabe, die öffentlichen Schlüssel zu verteilen. Näheres wird in der *Policy* vereinbart. Die *Policy,*[10] die in enger Abstimmung mit dem Datenschutzbeauftragten erstellt wurde, legt das Regelwerk fest, in welchem Rahmen die Zertifizierungsstelle arbeitet und die Anwender den Datenaustausch durchführen können. Nach akzeptablen Ergebnissen kann, so die Planung, die Teilnehmernahl sukzessive ausgebaut werden.

---

[7] Über die Leistungen von X.400 vgl. L. *Hertweck:* X.400: Einsatzbereiche, Sicherheitsfeatures und Architektur. In: iX. Heft 4. 1997. S. 140 ff.

[8] *Hessen-media.* Projektdokumentation. Hg. von der Hessischen Staatskanzlei (Schriftenreihe der Landesinitiative Hessen-media 1). Wiesbaden 1997. liefert einen Überblick über die derzeit landesweiten digitalen Multimedia-Projekte und Informationsdienste.

[9] In einem Diskussionspapier als Vorlage für die UABA-Sitzung vom 9. Juli 1997 stellte die HZD im Juli 1997 die Leistungen von X.400 systematisch denen des Internets gegenüber. Das Ergebnis dieser Betrachtung war eindeutig: Sollte mit dem kostengünstigeren Internet eine X.400 vergleichbar sichere Datenübermittlung möglich sein, so bestünde kein Grund, Internet nicht vermehrt zu nutzen. Auch der Leitfaden Sicherheit für Benutzer der Internet-Technologie. Hg. vom Forschungsinstitut für anwendungsorientierte Wissensverarbeitung (FAW) an der Universität Ulm. 1997. kommt, unter Beachtung bestimmter Regeln, zu einer positiven Bewertung der Verschlüsselungsverfahren. Der Leitfaden ist beziehbar über die Stabstelle für Verwaltungsreform beim Innenministerium des Landes Baden-Württemberg.

[10] Vorlage für die UABA-Sitzung vom 27. Februar 1998.

Der Pilotversuch soll insbesondere Erkenntnisse liefern über

- die Frage der Integration der Verschlüsselungskomponenten in die gängigen Mail-Systeme in der Landesverwaltung (derzeit X.400, MS-Mail, Outlook, Internet-Browser, Lotus Notes etc.) sowie die direkte Einbindung in Office-Produkte,
- die Aspekte des Anwendungskomforts (Automatisierung des Ver-/Entschlüsselungsvorgangs, leichter Zugriff auf die öffentlichen Schlüsselteile der Adressaten),
- die sichere Handhabung des privaten Schlüssels (Diskette, Aktivierung über Mantra),
- die Nutzung der Sicherheitskomponenten auf lokalen Systemen.

Die HZD ging zum Zeitpunkt der Antragstellung von einer maximalen Projektdauer von sechs Monaten aus. Mitte September 1997 stimmte der Landesautomationsausschuß diesem Antrag zu.[11]

Hinsichtlich des Verschlüsselungsverfahrens hat man sich für PGP (*Pretty Good Privacy*) entschieden, bei dem asymmetrische Schlüssel eingesetzt werden.[12] Will ein Anwender eine Datei versenden, so muß er diese Datei mit dem auf dem Key-Server zugänglichen öffentlichen Schlüssel des Adressaten verschlüsseln, damit nur und ausschließlich der Empfänger mit seinem privaten Schlüsselteil die Datei wieder entschlüsseln, also lesen kann. Desweiteren ist die Überprüfung der authentischen Herkunft der Daten mittels des Hashings möglich. Das Verfahren ist recht einfach: Der Absender bildet von seiner Datei mit Hilfe seines geheimen Schlüssels ein Hash-Komprimat, eine spezifische Quersumme, und sendet Ursprungsdatei plus Hash-Komprimat verschlüsselt an den Empfänger. Dieser entschlüsselt die erhaltene Datei und erhält Ursprungsdatei plus Hash-Komprimat. Anhand des öffentlichen Schlüssels des Absenders kann er nun von der Ursprungsdatei ein weiteres Hash-Komprimat erzeugen. Stimmt dieses mit dem von dem Absender übermittelten vollständig überein, sind die Daten in dem gleichen Zustand wie vor der Bildung des ersten Komprimats, also authentisch.

Ein detaillierter Erfahrungsbericht über das Pilotprojekt kann an dieser Stelle nicht geliefert werden, da es noch nicht abgeschlossen ist und erst eine kleine Testgemeinde ausgestattet wurde. Nach Befragungen im Kreise der Projektteilnehmer zeichnen sich aber Tendenzen ab.

Bisher entsprach es der Philosophie fast aller Behörden, zwar IT innerhalb des eigenen Hauses zu entwickeln und auszubauen, die Außenkontakte übernahmen aber fast regelmäßig einzelne Gateway-Rechner oder Modem-Stationen. Sicherheitsgründe waren hierfür maßgeblich, Ziel war der Schutz vor Viren und vor Einbruch von außen ins eigene Netzwerk (Stichwort *Firewall*). Datenaustausch von Dienststelle zu Dienststelle gehört selbstverständlich zu den Zielen des IT-Einsatzes; daran, daß einzelne Mitarbeiter in das WWW gingen, war bisher aber kaum gedacht. Erst in jüngster Zeit wurde das Internet auch für die Landesbehörden interessant, und es wurden vermehrt Anschlüsse eingerichtet. Dem Sicher-

[11] Protokoll der 210. LAA-Sitzung vom 16. September 1997.

[12] Stellvertretend für zahlreiche Informationsmöglichkeiten über PGP im Internet wie in Fachzeitschriften der Leitfaden Sicherheit für Benutzer der Internet-Technologie, wie Anm. 9.

Gegen Ende der ersten Jahreshälfte, nach Überwindung der technischen Probleme im Testbetrieb, wird man sich, so die Prognose, konkrete Gedanken über die Frage machen können, welche Vorgänge auf diesem Wege bearbeitet werden können.

Welchen Einfluß haben die geschilderten Entwicklungen auf die Archivierung von Unterlagen aus digitalen Systemen?

Bei allen Anwendern der kryptographischen Verfahren steht im Vordergrund der Bemühungen, Informationen schnell, sicher und authentisch zu übermitteln. Ziel ist es, die Bearbeitungszeiten innerhalb der (eigenen) Verwaltung entscheidend zu verkürzen; weit nachgeordnet und im Vergleich unerheblich ist die Perspektive der Personaleinsparung. Das papierlose Büro ist einstweilen noch in weiter Ferne – in einigen Verwaltungen schon allein aufgrund der Tatsache, daß der IT-Ausbau noch nicht vollständig abgeschlossen ist. Allerdings wird durchaus in einzelnen Referaten oder Abteilungen an die Abwicklung von Standardvorgängen mit Formularcharakter über IT, etwa im Bereich der inneren Verwaltung gedacht – zum Beispiel die Genehmigung von Urlaubsanträgen o.ä. In anderen Bereichen ist denkbar, die Materialverwaltung elektronisch zu unterstützen und dabei das Einkaufs-, Bestell- und Rechnungswesen einzubeziehen.

Es gibt aber auch Verwaltungen, die bereits über gut ausgebaute Infrastrukturen verfügen, welche den Datenaustausch nicht nur hausintern, sondern auch zwischen vorgesetzter und nachgeordneten Behörden unterstützen. Bisher wurden hier insbesondere X.400 und/oder Modem eingesetzt. Beide Systeme waren aber noch nicht für die Versendung sensibler Daten vorgesehen, eine Verschlüsselung – gleich ob in X.400 oder über Internet-e-mail – würden hier endlich den Weg für die Übermittlung vertraulicher Informationen freigeben, was die Kommunikation mit den Außenstellen wie auch mit anderen Dienststellen erheblich erleichtern wird.

Interessant wird verschlüsselte e-mail insbesondere dort, wo die Ablaufkonzeption behördenintern bereits auf weitgehenden Einsatz von IT aufsetzt – wo etwaige Hauserlasse schon zwischen *offiziellem*, papiergestütztem Geschäftsgang und *sonstiger*, möglichst zu nutzender elektronischer Informationsübermittlung unterscheiden und gegebenenfalls bereits Registraturprogramme existieren, die eine elektronische Archivierungskomponente (Altablage) beinhalten. Hier ist der Weg zum papierlosen Büro rein technisch nicht mehr weit. Es fehlen nurmehr echte Workflow-Umgebungen und ein internes Konzept zum Nachweis der authentischen Bearbeitung eines Vorgangs durch einen bestimmten Mitarbeiter, etwa unter Verwendung eines persönlichen Schlüsselcodes.

Im Hinblick auf die Schriftgutproduktion läßt sich abschließend folgendes Fazit ziehen:

Besonders geeignet für die Übertragung auf digitale Systeme sind – nach wie vor – gleichförmige, formularmäßige Bearbeitungsvorgänge. Im großen Stil wird hier IT schon seit Jahrzehnten eingesetzt, jeder kennt Beispiele zur Genüge. Ob bei den zentralen Landesbehörden die archivische Bewertung in Bälde ernsten Problemen gegenübersteht, darf bezweifelt werden; tendenziell dürfte insbesondere das ohnehin kassable, routinemäßige verwaltungsinterne Schriftgut betroffen sein. Anders sieht es selbstverständlich bei einigen Fachverwaltungen aus, die strukturell in starkem Maße serielles Schriftgut erzeugen oder mit großen Datenbanken arbeiten, wie etwa das Statistische Landesamt, die Kataster- oder Grund-

heitsbedürfnis der Landesverwaltung gegen Viren trug man Rechnung, indem die Internet-Zugänge für die Landesbehörden über einen speziellen Server bei der HZD geleitet werden, der die Firewall-Funktion zentral gewährleistet.[13]

Welche unterschiedlichen Ausgangslagen trifft das Verschlüsselungsprojekt nun konkret an?

Die Situation kann in einem Ministerium zum Beispiel so aussehen, daß X.400 auf einem Gateway zur Verfügung steht. In einem anderen wird es auch als internes Mail-System genutzt. Abgesehen von einer vertretbaren monatlichen Pauschale verursacht X.400 weder im hausinternen Betrieb noch bei der landesweiten Nutzung (inclusive Hessische Landesvertretung in Bonn) über die HZD weitere Kosten. Erhebliche Beträge fallen aber an, wenn Daten bundesweit oder gar international übermittelt werden. Selbstredend tangiert dieses Problem die einzelnen Verwaltungen unterschiedlich: Im Ministerium für Jugend, Familie und Gesundheit etwa wird dieser Nachteil kaum wahrgenommen, im Kultusministerium hingegen angesichts des hohen bundesweiten Koordinierungsbedarfs schon viel stärker. Ein lästiges Problem gerade bei der Übermittlung von Daten außer Haus sind bei X.400 die komplizierten Adressen, die fehlerfrei eingegeben werden müssen. Für den hausinternen Gebrauch können die Adressen allerdings vereinfacht dargestellt werden, so daß X.400, etwa in Exchange eingebunden, den üblichen Komfort bietet, also im wesentlichen per Mausklick funktioniert.

Die öffentlichen Verwaltungen sehen sich nun aber der Tatsache gegenüber, daß immer mehr Korrespondenzpartner e-mail per Internet nutzen. Insofern besteht schon seit längerem verstärktes Interesse, daß die HZD einen Gateway-Rechner zur Verfügung stellt, der X.400 und Internet-e-mail unterstützt.[14] Eine solche Lösung ist insbesondere auch deshalb für die Nutzer der Datenübermittlung attraktiv, weil X.400 aufgrund datensicherheitstechnischer Aspekte absehbar nationaler und europäischer Behörden-Standard bleiben wird und daher unverzichtbar ist. Dennoch kann offenbar niemand die Augen vor dem Internet verschließen. Abgesehen vom kostengünstigen Anschluß ergibt sich so kraft des Faktischen für die hausinternen Netze die notwendige Folge, zunächst zumindest einzelne Anwendungen, insbesondere natürlich Textverarbeitung und e-mail, sukzessive auf entsprechende Standards, derzeit v.a. Windows-NT, umzustellen – und natürlich erwarten die Anwender in beiden Welten den gleichen gewohnten Komfort und die gleichen Nutzungsmöglichkeiten, insbesondere in puncto Datenübertragungssicherheit.

Im Fall einer landesweiten Fachverwaltung mit einem Dutzend Außenstellen wird die Verwendung von PGP bereits für den geplanten Ausbau eines landesweiten Netzes ins Auge gefaßt. Dort wird lokal Lotus Notes eingesetzt, das netzintern ebenfalls die Verwendung von öffentlichen und privaten Schlüsseln anbietet. Die Kommunikation zwischen den Außenstellen soll nun so aussehen, daß grundsätzlich alle PC-Stationen mit öffentlichen und privaten Schlüsseln versorgt werden und Kommunikation und Vorgangsbearbeitung landesweit möglich wird. Die Datenübermittlung soll über PGP-verschlüsselte e-mail im Internet bewerkstelligt werden. Die öffentlichen Schlüssel werden für alle Nutzer zugänglich gehalten.

[13] „Unterhalb" dieses Servers wird derzeit an der Einrichtung eines Landes-Intranets gearbeitet.

[14] Vgl. Vorlage Gateway X.400 <-> SMTP für die UABA-Sitzung vom 27. Februar 1998.

buchverwaltung.[15] Angesichts breiter Nutzung des Internets in kommerziellen Bereichen wie Home-Banking oder Tele-Shopping – ebenfalls Dienste, die auf der absoluten Zuverlässigkeit der Datenübertragungswege wie auch der Sicherheit hinsichtlich der Authentizität der abgesandten Daten angewiesen sind –, darf man sich keiner Illusion hingeben: Zukünftig werden solche Anwendungen auch bei öffentlichen Dienstleistungen eine Rolle spielen. In Hessen beispielsweise existiert bereits ein Projekt zur elektronischen Steuererklärung.[16]

Die entscheidende, eingangs angeschnittene Frage ist, wie das charakteristische Schriftgut der zentralen Landesbehörden, die differenzierte Sachakte, in einigen Jahren aussehen wird. Die Perspektiven stehen nun in etwas klareren Konturen vor uns: Sind die technischen Probleme der Krypto-Verfahren ausgeräumt, wird sehr bald eine Infrastruktur installiert werden, die den vertraulichen Datenaustausch zwischen den Dienststellen des Landes ermöglicht. Zweifellos wird die Zahl der Teilnehmer an diesem Netz rasch zunehmen,[17] und diese Teilnehmer sind dann definitiv in der Lage, die Vorgangsbearbeitung digital zu erledigen. Noch denkt niemand laut über die Abschaffung der differenzierten Sachakte in Papierform und deren Führung in rein digitaler Form nach. Die Verwaltung weiß, was sie an ihren dokumentenechten, Rechtssicherheit gewährleistenden Schriftstücken in schwarz auf weißem Papier hat. Dennoch ist angesichts der rasanten Veränderungen im Bereich der Bürokommunikation Wachsamkeit gefordert, denn prinzipiell steht der Umstellung auch von Sachakten in Papierform auf digitale Akten in der hessischen Landesverwaltung weder technisch noch rechtlich etwas im Wege.[18] Patentrezepte für den Umgang mit diesen Veränderungen für die Archive können nicht geliefert werden.[19] Spätestens bei der Einrichtung von elektronischen Archivierungskomponenten in den Behörden müssen sie sich einschalten.

---

[15] Zunehmende Bedeutung haben hier auch die elektronischen Informationsdienste.

[16] Vgl. *Hessen*-media, wie Anm. 8, S. 75.

[17] Hierfür spricht, daß nach Beobachtung von Systembeauftragten die Attraktivität von e-mail deutlich zunehme, seitdem dies mit Internet-Zugang in Verbindung steht – nicht weil die Teilnehmer das Netz für private Zwecke nutzen wollten, aber die Schwellenängste seien erheblich niedriger und die Reputation in der Öffentlichkeit besser als die behördeninterner Systeme.

[18] Der hier maßgebliche Gemeinsame Erlaß des Hessischen Ministeriums des Innern, des Ministeriums für Landwirtschaft, Forsten und Naturschutz und des Hessischen Ministeriums der Finanzen vom 4. Dezember 1996 über Aufbewahrungsbestimmungen für Akten und sonstiges Schriftgut der Dienststellen des Landes Hessen. In: Der Archivar 50 (1997) Sp. 783–795. bestimmt unter Punkt 13.1 über die Aufbewahrungsfristen im Rahmen elektronischer Datenverarbeitung: *Datenträger und Bildträger, die konventionell geführte Bücher, Belege [...] oder Akten ersetzten oder ergänzen einschließlich der dazugehörigen Programme, Programmakten, Arbeitsanleitungen und sonstige schriftlichen Unterlagen sind Akten im Sinne dieses Erlasses. Die Lesbarkeit von verfilmten oder elektronisch gespeicherten Daten ist für die Aufbewahrungszeit sicherzustellen.*

[19] Den Schlußfolgerungen für die Archive, wie sie Michael *Wettengel*, wie Anm. 1, S. 18–20. formuliert, ist nur zuzustimmen.