**Wolfgang Farnbacher,**
**Vom Posteingang bis in das Archiv**
Technische und organisatorische Konzepte des ArchiSig-Projekts

aus:

Digitales Verwalten – Digitales Archivieren

Veröffentlichungen aus dem Staatsarchiv der Freien und Hansestadt Hamburg, Band 19

Herausgegeben von Rainer Hering und
Udo Schäfer

S. 51-66

## Impressum für die Gesamtausgabe

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Diese Publikation ist außerdem auf der Website des Verlags Hamburg University Press *open access* verfügbar unter http://hup.rrz.uni-hamburg.de.

Die Deutsche Bibliothek hat die Netzpublikation archiviert. Diese ist dauerhaft auf dem Archivserver Der Deutschen Bibliothek verfügbar unter http://deposit.ddb.de.
ISBN 3-937816-09-7 (Printausgabe)
ISSN 0436-6638 (Printausgabe)

# Inhalt

## Dokumentenmanagementsysteme (DMS) zwischen Verwaltung und Archiv

# Vom Posteingang bis in das Archiv

## Technische und organisatorische Konzepte des ArchiSig-Projekts

Wolfgang Farnbacher

200 Millionen Seiten Papier werden nach einer Berechnung der niedersächsischen Archivverwaltung jedes Jahr allein in der niedersächsischen Landesverwaltung zu den Akten genommen und dann im Durchschnitt 10 Jahre lang aufbewahrt. Würde man dieses Papier aneinander gereiht in Regale stellen, ergäbe sich eine Regalbreite von ungefähr 20 Kilometern. Über die Anzahl der verbindlichen Unterschriften auf diesen Dokumenten gibt es keine verlässlichen Angaben. Nimmt man jedoch eine Unterschriftsrate von nur 1 Prozent an, verbleiben immerhin noch 2 Millionen signifikante Unterschriften pro Jahr. Diese Dokumente werden nach Abschluss der laufenden Verfahren im Durchschnitt ca. 10 Jahre aufbewahrt, bevor sie der niedersächsischen Archivverwaltung zur dauerhaften Aufbewahrung angeboten werden. Diese übernimmt ca. 5 Prozent des angebotenen Aktenbestandes, jährlich immerhin noch eine Regallänge von einem Kilometer. Nun wird selbst durch die Einführung einer Vielzahl von E-Government-Verfahren dieser Papierberg nicht plötzlich verschwinden. Die Ablösung vollzieht sich langsam. Papier wird noch über Jahre das überwiegende Arbeitsmedium in der Verwaltung (und natürlich auch in den anderen gesellschaftlichen Bereichen) sein. Zu merken ist der Wechsel aber schon heute. Tausende E-Mails passieren den zentralen Mailserver des Informatikzentrums Niedersachsen täglich (dienststelleninterner Mailverkehr nicht mitgezählt), unzählige Dokumente werden auf den PC-Arbeitsplätzen von den Sachbearbeitern elektronisch erstellt. Heute werden sie am Ende allerdings immer noch ausgedruckt und dann in Akten geheftet.

Der angestrebte Wandel von der papierorientierten zur weitgehend elektronisch unterstützten Aufgabenerledigung wird auf allen Ebenen der öffentlichen Verwaltung und Justiz tief greifende Veränderungen mit sich bringen. Zahlreiche E-Government-Initiativen von Bund, Ländern und Kommunen beinhalten immer wieder zwei Schlüsseltechniken beziehungsweise deren praxisgerechten Einsatz: die elektronische Signatur, die an die Stelle herkömmlicher Unterschriften tritt, und die elektronische Aktenführung, die die herkömmlichen Papierakten ersetzen soll. Wie jedoch mit den gegenüber Papierdokumenten in Form und Darstellung so völlig andersartigen Unterlagen aus der digitalen Welt angemessen umzugehen ist, ist ein in vielen Teilen noch unbeantworteter Fragenkomplex.

Die Niedersächsische Staatskanzlei hat dies schon frühzeitig erkannt und beteiligt sich mit Unterstützung des Informatikzentrums Niedersachsen daher an dem Projekt „ArchiSig – beweiskräftige und sichere Langzeitarchivierung digital erzeugter und signierter Dokumente“. In dem E-Government-Projekt „Langzeitarchivierung“, getragen von der Niedersächsischen Staatskanzlei (staatliche Archivverwaltung) und dem Informatikzentrum Niedersachsen, werden nun die Ergebnisse aus dem Projekt ArchiSig prototypisch in die niedersächsische Infrastruktur integriert und für die öffentliche Verwaltung praxisgerecht umgesetzt.

In der Praxis gibt es vier wesentliche Problemfelder, die bei der langfristigen beweiskräftigen Aufbewahrung elektronisch signierter Dokumente betrachtet werden müssen.

## 1 Welche Signatur- und Dokumentformate ermöglichen überhaupt eine langfristige Aufbewahrung?

Da es eine unüberschaubare Vielzahl von Dokumentenformaten am Markt gibt, aber nur Anwendungen für eine begrenzte Anzahl von Formaten in der öffentlichen Verwaltung vorhanden sein können, muss eine Festlegung akzeptierter Dokumenten- beziehungsweise Dateiformate auf der Basis bestehender Rechtsvorschriften und fachlicher Anforderungen durchgeführt werden.

Um ein Datenformat für die Langzeitspeicherung elektronisch signierter Dokumente einsetzen zu können, wird gefordert, dass es keinen häufigen

Änderungen der Datenstruktur und damit Versionswechseln unterliegt, was als Stabilität eines Datenformates bezeichnet wird. Ein Datenformat muss auch noch nach Jahren interpretiert werden können, und häufige Versionswechsel erschweren die Verarbeitung von Dokumenten in älteren Formatversionen. Werden bei neuen Formatversionen nicht nur Erweiterungen vorgenommen, sondern auch Änderungen der Datenstruktur, so werden die Präsentation und Verifikation von älteren Dokumenten mit aktueller Software zum Teil unmöglich. Ein wichtiges Kriterium für die Bewertung ist auch die Transparenz eines Datenformates. Man spricht von einem transparenten Datenformat, wenn seine Spezifikation vollständig offen gelegt ist, das heißt, wenn eine vollständige Spezifikation frei verfügbar ist. Das ist bei so genannten De-jure-Standards der Fall, die von öffentlichen Standardisierungsgremien wie zum Beispiel der International Organization for Standardization (ISO) festgelegt werden. Bei Industriestandards, die auch als De-facto-Standards bezeichnet werden, sind die Spezifikationen nur zum Teil offen gelegt.

Im Bereich der Dokumentformate werden in der niedersächsischen Landesverwaltung derzeit die Formate TIFF (Tagged Image File Format) und mit Einschränkung PDF (Portable Document Format) empfohlen. Die Entwicklung weiterer Formate wie zum Beispiel PDF-A[1] und solcher auf XML-Basis wird beobachtet.

Da eine elektronische Signatur untrennbar mit dem dazugehörigen Dokument verbunden ist, gelten die Anforderungen, die an Dokumentformate gestellt wurden, im gleichen Maße auch für die eingesetzten Signaturformate. Die Analysen der Signaturdatenformate haben gezeigt, dass für alle Verifikationsdaten und allgemeinen Signaturformate international anerkannte Standards mit offen gelegten Spezifikationen existieren. Fast alle Spezifikationen wurden allerdings erst innerhalb der vergangenen fünf Jahre entwickelt, weshalb sich über deren Stabilität keine gesicherten Aussagen machen lassen. Eine eindeutige Empfehlung für den Einsatz eines

[1] PDF-A ist ein Format auf PDF-Basis, welches für die Langzeitarchivierung optimiert wird; das Format soll nach ISO normiert werden. Siehe www.aiim.org/standards.asp?ID=25013 (Stand: Mai 2004).

bestimmten Signaturformats kann an dieser Stelle daher nicht ausgesprochen werden.

Insgesamt kann festgestellt werden, dass derzeit kaum Dokument- und Signaturformate existieren, die allen Kriterien umfassend gerecht werden. Durch die ständige Weiterentwicklung ist derzeit keine Stabilität gewährleistet, und die Datenformate können in 30 Jahren gegebenenfalls nicht mehr interpretiert werden. Sicherheitsmechanismen wie elektronische Signaturen werden von den Nutzdatenformaten nur zum Teil unterstützt, und die Problematik der nachlassenden Beweiskraft elektronisch signierter Dokumente über Aufbewahrungszeiträume von 30 und mehr Jahren wird bislang nur unzureichend berücksichtigt. Es ist aber auch festzustellen, dass die Diskussion fortschreitet und Aspekte der langfristigen Aufbewahrung zunehmend an Bedeutung gewinnen.

Wenig beachtet bei der Diskussion um Dokument- und Signaturformate wurde bisher die Tatsache, dass auch die Verifikationsdaten einer Signatur (also die Daten einer Gültigkeitsprüfung zum Zeitpunkt der Signaturerstellung) einem Alterungsprozess unterliegen. Zur Verifikation von Signaturen sind neben den eigentlichen Signaturen (das heißt verschlüsselten Hashwerten beziehungsweise den Signaturwerten) zusätzliche Daten erforderlich. Dies sind insbesondere Zertifikate, Ergebnisse von Zertifikats-Statusabfragen und Zeitstempel. Bei einer Verifikation zeitnah zur Signaturerzeugung können diese Daten zumeist aktuell und online beschafft werden. Sollen die Dokumentsignaturen nach langer Aufbewahrungszeit verifiziert werden, so muss jedoch damit gerechnet werden, dass Online-Verzeichnisse nicht mehr existieren oder dass die erforderlichen Daten mittlerweile gelöscht wurden. Um das Problem zu vermeiden, sollte versucht werden, Signaturen zu verwenden, für die sichergestellt ist, dass erforderliche Verifikationsdaten während der gesamten Aufbewahrungszeit der Dokumente beschaffbar sind. Dem steht jedoch wiederum entgegen, dass der Empfänger eines signierten Dokumentes die vom Signierer verwendeten Signaturen nicht immer bestimmen kann, dass langfristig nicht sicher vorhersagbar ist, ob Zertifizierungsdiensteanbieter heute gegebene Versprechungen auch einhalten können und dass es für den Fall von ewig aufzubewahrenden Dokumenten mit Sicherheit keine ewig verfügbaren Zertifizierungsdienste geben wird. Deshalb müssen geeignete Archivierungssysteme ergänzend die Möglichkeit bieten, erforderliche Verifikationsdaten aufzubewahren. Die Aufbewahrung muss berück-

sichtigen, dass die Verifikationsdaten Signaturen enthalten können, deren Algorithmen ihre Sicherheitseignung verlieren. Systeme, die signierte Dokumente archivieren, müssen über Komponenten verfügen oder Services ansteuern können, die eine beweiskräftige Aufbewahrung ermöglichen.

## 2 Wann müssen die Maßnahmen zur langfristigen Aufbewahrung eigentlich beginnen?

Eine der wesentlichen Erkenntnisse des ArchiSig-Projekts ist die Feststellung, dass der gesamte Lebenszyklus elektronischer Dokumente in den Blick genommen werden muss, angefangen bei ihrer ersten Erzeugung beziehungsweise Annahme in Dokumentenmanagementsystemen und elektronischen Poststellen über ihre sichere Aufbewahrung in Langzeitspeichern bis hin zur dauerhaften Erhaltung in einem elektronischen Staatsarchiv. Nur so ist das Ziel der Schaffung einer sicheren Infrastruktur als Basiskomponente für alle elektronischen Dienstleistungen zu erreichen. Eine Beschränkung auf den letzten Lebensabschnitt eines Dokuments reicht nicht aus.

Zur Erreichung dieses Ziels muss eine Eingangs- und Ausgangsinfrastruktur für elektronisch signierte Dokumente und für Papierdokumente, die in eine sichere elektronische Form beziehungsweise umgekehrt transformiert werden müssen, aufgebaut werden. Hier müssen vor allem organisatorische und technische Regeln für den Umgang mit elektronischen Dokumenten, die eine Behörde über den E-Mail-Weg erreichen, geschaffen und praktisch erprobt werden. Benötigt wird die Funktionalität, eingehende Sendungen (E-Mails) auf formale Korrektheit zu überprüfen und weiterzuleiten beziehungsweise zu verteilen oder bei Nichterfüllung der Annahmekriterien an den Absender zurückzusenden und diesen entsprechend zu informieren. Diese Vorgänge müssen automatisiert ablaufen. Das Problem des Umgangs mit weiterhin vorhandenen Papierdokumenten wird an anderer Stelle dieses Artikels noch einmal gesondert behandelt.

Ein weiterer Bereich mit Handlungsbedarf ist die sichere Ausgestaltung von Dokumentenmanagementsystemen (DMS) und bereichsspezifischen Fachanwendungen mit vergleichbarer Funktionalität für den Umgang mit elektronisch signierten Dokumenten und Dokumentensammlungen. Schwerpunkt ist dabei die grundsätzliche Festlegung von Anforderungen an die

elektronische Abbildung von Akten und Vorgängen als rechtssicherer und praxistauglicher Ersatz für entsprechende Papierversionen. Um die Notwendigkeit festzustellen, Dokumente mit elektronischen Signaturen zu versehen und die elektronischen Signaturen über längere Zeiträume zu erneuern, müssen sie zunächst nach ihrer juristischen Bedeutung klassifiziert werden. Ein förmlicher Beweisbedarf von elektronisch erstellten und langzeitgespeicherten Dokumenten besteht im Wesentlichen bei gerichtlichen Verfahren zur Überprüfung einer Verwaltungsentscheidung und bei Maßnahmen zum Vollzug von rechtskräftigen Verwaltungsentscheidungen. Obwohl die Überprüfung einer Verwaltungsentscheidung durch die Festsetzung von Fristen zur Rechtsmittelwahrung prinzipiell zeitnah erfolgen sollte, spielt die Verfahrensdauer von gerichtlichen Überprüfungen in der Praxis eine zunehmende Rolle. Die Dauer von gerichtlichen Verfahren nimmt bei Rechtsstreitigkeiten über mehrere Instanzen stark zu. Verfahren mit einer Dauer von mehr als 10 Jahren sind keine Seltenheit mehr, selbst einfache Verfahren können aus vielerlei Gründen die Gültigkeitsdauer einer elektronischen Signatur überschreiten. Da Verwaltungshandeln im Gegensatz zum Zivilrecht häufig Ermessensentscheidungen beinhaltet, sind bis zur Rechtskraft einer Entscheidung grundsätzlich alle Dokumente (Informationen) eines Vorgangs rechtlich relevant. Auch für solche Dokumente, die für sich eigentlich keiner elektronischen Signatur bedürfen, muss daher auf jeden Fall die Authentizität und Integrität für die Verfahrensdauer sichergestellt sein. In dem niedersächsischen E-Government-Projekt „Langzeitarchivierung“ wird daher versucht, Entscheidungshilfen zu definieren, ob und gegebenenfalls. in welchen Fällen ein internes Mitzeichnungsverfahren den Einsatz einer elektronischen Signatur mit entsprechender Beweiswerterhaltung der Mitzeichnung erfordert. Alternativ ist (wie in konventionellen DMS-Systemen) der Einsatz von datenbankgestützten Mitzeichnungsverfahren denkbar. Für beide Fälle muss festgelegt werden, in welcher Form die Mitzeichnung in einer elektronischen Akte zuverlässig dokumentiert wird. Die bisherige Form der Speicherung in DMS-spezifischen Datenbanktabellen beziehungsweise -sätzen erscheint für eine längerfristige Aufbewahrung nicht geeignet. Für die Behandlung der einzelnen Dokumentklassen sind automatisierte Abläufe zu definieren. Da heute eingesetzte kurzlebige Dokumentformate wie zum Beispiel MS-Word für eine längerfristige Aufbewahrung nicht geeignet erscheinen, muss die

Möglichkeit der Verwaltung eines Dokuments in zwei unterschiedlichen Formaten berücksichtigt werden. In der Praxis bedeutet dies, dass zunächst Arbeitsversionen mit einem gängigen Textverarbeitungsprogramm erstellt und bearbeitet werden, diese aber dann vor der elektronischen Signatur in ein dauerhaftes signierfähiges Format umgewandelt werden müssen (zum Beispiel Verwaltung einer Arbeitsversion im MS-Word-Format mit dazugehörigen signierten PDF- oder TIFF-Versionen).

## 3 Welche technischen Vorkehrungen müssen während des Aufbewahrungszeitraums getroffen werden?

Wie bereits festgestellt, sind Signaturen nicht unbegrenzt *haltbar*. Deshalb ist im Rahmen des ArchiSig-Projekts ein Konzept entwickelt worden, das über einen so genannten Archivzeitstempel eine Erneuerung von Signaturen, die zu veralten drohen, ermöglicht. Eine Grundlage dieses Archivzeitstempels sind Hashbäume.[2] Dieses Prinzip soll anhand von drei Abbildungen hier kurz erläutert werden.

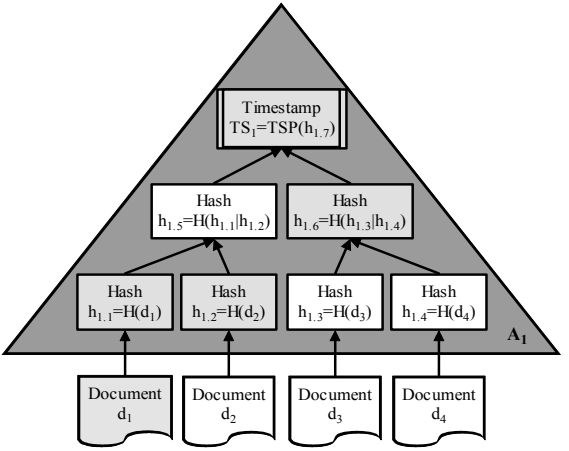


Abbildung 1

[2] Siehe Ralph Charles Merkle: Protocols for Public Key Cryptosystems. In: IEEE Symposium on Security and Privacy 1980. Oakland, CA, 1980. S. 122–134.

Die Blätter des in der Abbildung 1 dargestellten Archivzeitstempels stellen die Hashwerte von signierten Dokumenten oder beliebigen anderen Datenobjekten dar. Darüber liegende Hashwerte werden über die Folge der Sohnknoten gebildet. So wird beispielsweise der Hashwert $h_{1.5}$ gebildet, indem die Hashwerte $h_{1.1}$ und $h_{1.2}$ konkateniert und dann erneut gehasht werden. Für den Wurzel-Hashwert wird ein Zeitstempel von einem akkreditierten Zertifizierungsdiensteanbieter eingeholt, der eine akkreditierte Signatur trägt. Der Wurzel-Hashwert des Hashbaumes ist im Zeitstempel selbst enthalten und wird deshalb nicht aufgeführt. Durch einen Archivzeitstempel können beliebig viele signierte Dokumente über einen Zeitstempel gesichert werden, ohne den Aufwand zur Erzeugung oder Prüfung deutlich zu erhöhen. Dabei ist die Löschung beliebiger, durch einen Archivzeitstempel gesicherter Dokumente möglich, ohne den Beweiswert anderer zu beeinträchtigen.

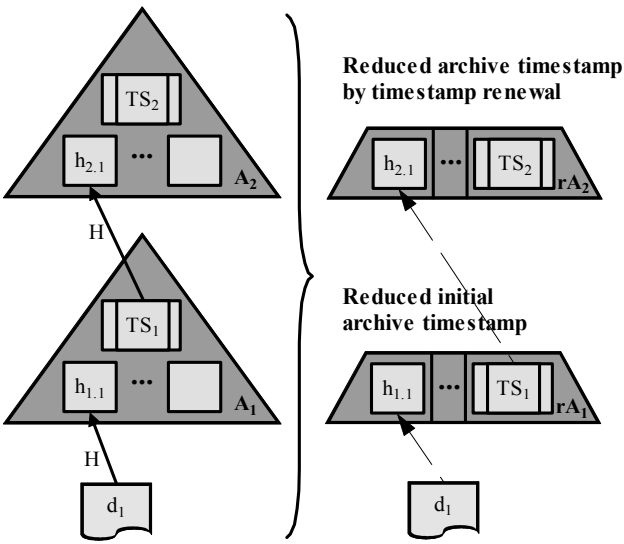


Abbildung 2

Die Zeitstempel-Erneuerung wird durchgeführt, bevor einer der im Zeitstempel (das heißt der Zeitstempelsignatur und ihren Verifikationsdaten) verwendeten Hash- oder Public-Key-Algorithmen oder zugehörigen Parameter unsicher wird, aber der im Hashbaum verwendete Hash-Algorithmus noch sicher ist. Bei der Zeitstempel-Erneuerung wird der Zeitstempel eines Archivzeitstempels in einen neuen Archivzeitstempel einbezogen.

Dabei wird, wie in Abbildung 2 veranschaulicht, der Hashwert des Zeitstempels $TS_1$ gebildet und als Blatt $h_{2.1}$ in den Hashbaum des neu zu bildenden Archivzeitstempels eingefügt. Dabei ist der bisherige, noch sicherheitsgeeignete Hash-Algorithmus H anzuwenden.

Der durch Zeitstempel-Erneuerung entstandene Archivzeitstempel kann für ein signiertes Dokument ebenfalls auf wenige Hashwerte und einen Zeitstempel reduziert werden. Dieser reduzierte Archivzeitstempel $rA_2$ kann dann im rechtlichen Sinne als zweite erneute Signatur für das signierte Dokument gelten. Die Zeitstempel-Erneuerung ist effektiv und kostengünstig durchführbar. Es muss nur auf betroffene Archivzeitstempel zugegriffen werden, nicht aber auf die durch diese referenzierten Dokumente. Zur Erneuerung einer beliebigen Anzahl unsicher werdender Archivzeitstempel ist nur ein einziger neuer Archivzeitstempel erforderlich und mithin nur ein Zeitstempel. Die einfache Zeitstempel-Erneuerung kann so lange wiederholt werden, wie nur Algorithmen unsicher werden, die im Zeitstempel verwendet wurden. Erst wenn der im Hashbaum verwendete Hash-Algorithmus unsicher wird, muss ein aufwändigeres Erneuerungsverfahren durchgeführt werden.

Bei dieser Hashbaum-Erneuerung müssen, wie in Abbildung 3 dargestellt, neben unsicher werdenden Archivzeitstempeln auch die durch sie referenzierten signierten Dokumente berücksichtigt werden.

Hier sieht ArchiSig vor, das initial archivgestempelte Dokument und die zwischenzeitlich erzeugten reduzierten Archivzeitstempel ($rA_1$ und $rA_2$) mit einem neuen, sicherheitsgeeigneten Hash-Algorithmus H' zu hashen. Die Konkatenation der beiden erhaltenen Hashwerte bildet das Datenobjekt, das durch Hashwertbildung in einen neuen Archivzeitstempel einbezogen wird, der ebenfalls H' im Hashbaum verwendet. Auch dieser neue Archivzeitstempel $A_3$ lässt sich wiederum für das signierte Dokument reduzieren. Der so reduzierte Archivzeitstempel $rA_3$ ist dann die durch die Hashbaum-Erneuerung entstandene erneute Signatur des Dokuments. Durch zusätzliche Redundanzmechanismen, wie die Erzeugung von mehreren Archivzeit-

stempeln mit unterschiedlichen Hash-Algorithmen zu denselben Dokumenten, kann die Notwendigkeit der Hashbaum-Erneuerung aber minimiert oder eventuell sogar ganz vermieden werden.

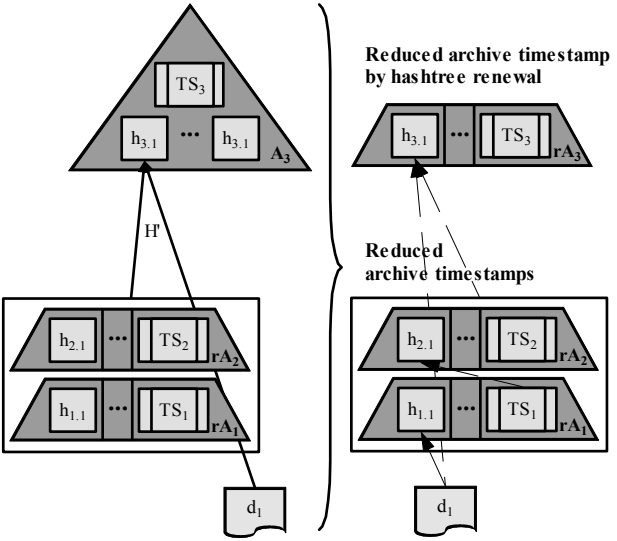


Abbildung 3

Mit dem vorgestellten Konzept sind Signaturen über einen langen Zeitraum hinweg beweiswerterhaltend zu erneuern. Bedingt durch die Hardwareentwicklung, wachsende Ansprüche an neue Medien, geänderte Geschäftspolitiken der Softwarehersteller, Harmonisierungsbestrebungen und auch neue rechtliche Vorgaben ändern sich mit der Zeit allerdings auch Nutzdaten- und Signaturdatenformate. Signaturspezifisch ist dabei allerdings, dass traditionelle Lösungen, wie die Konvertierung von Dokumenten, die Prüfbarkeit von Signaturen zerstören und deshalb den Beweiswert der Signaturen nicht erhalten. Es muss also versucht werden, Datenformate für signierte Dokumente und Signaturen zu verwenden, für die über die gesamte Archivierungsdauer erforderliche Programme zur Verifikation und Präsentation auf gängigen Plattformen verfügbar sein werden. Dem steht entgegen, dass

der Empfänger eines signierten Dokumentes die vom Signierer verwendeten Dokument- und Signaturformate häufig nicht bestimmen kann und dass langfristig schwer vorhersagbar ist, welche Formate sich dauerhaft durchsetzen werden. Deshalb muss es ergänzende Methoden geben, um elektronische Dokumente unter Beibehaltung ihrer rechtlichen Eigenschaften in andere, archivtaugliche Formate zu transformieren. Der Begriff „Transformation" wird in unterschiedlichsten Zusammenhängen verwendet und nicht immer einheitlich interpretiert. Allgemein wird darunter die Umwandlung eines in einem bestimmten (Ausgangs-)Format (digital oder analog) vorliegenden Dokuments in ein anderes (Ziel-)Format verstanden. Dabei sollen wesentliche Eigenschaften des Ausgangsdokuments erhalten bleiben. Die Begriffe Konvertierung und Transformation werden in Bezug auf die Umwandlung von Daten oft synonym verwendet. Der Begriff Transformation wird im Rahmen des ArchiSig-Projekts und dieses Artikels so definiert, dass im Unterschied zur Konvertierung das Ziel- oder das Quelldokument oder beide mit einer qualifizierten Signatur, besser einer qualifizierten Signatur mit Anbieter-Akkreditierung (nachfolgend *akkreditierte Signatur*), versehen sein müssen beziehungsweise versehen werden. Außerdem soll das Verfahren die Dokumentinhalte erhalten und nachweisbar sicher sein, so dass die Beweiskraft der transformierten Dokumente sichergestellt ist.

Vereinzelt sind bereits gesetzliche Regelungen erlassen worden, die zur Sicherung der Transformationsergebnisse eine elektronische Beglaubigung vorsehen beziehungsweise bestimmen, wie der Ausdruck eines ursprünglich in elektronischer Form vorliegenden Dokuments bestätigt werden muss, um als beglaubigte Abschrift gelten zu können. Insgesamt befindet sich das Thema aus rechtlicher und technischer Sicht jedoch noch auf sehr dünnem Eis. Dies gilt insbesondere vor dem Hintergrund, dass bei einer *elektronisch beglaubigten Abschrift* gerade zum Zwecke der Vernichtung des Ursprungsdokuments ein Rückgriff auf das *Original* ausgeschlossen ist und die bestehenden prozessualen Regelungen auf Dokumente in Papierform ausgerichtet sind. Die einzelnen Regelungen sind daher im Licht ihrer materiell-rechtlichen und prozessualen Wirkung zu betrachten, wobei nach dem mit der Regelung verbundenen Zweck zu differenzieren ist. Hierbei ist immer zu berücksichtigen, dass nicht mit allen Vorschriften der Anspruch einer öffentlichen/amtlichen Beglaubigung geltend gemacht wird. Ein Lösungsvorschlag für die besondere Form der Transformation von Papierdo-

kumenten in eine elektronische Form wird jedoch zur Beantwortung der folgenden Frage beschrieben.

## 4 Wie kann die parallele Nutzung von Papierdokumenten und elektronischen Dokumenten vereinfacht werden?

Zu den wesentlichen Problemen in der Übergangszeit zwischen einer vorwiegend papierorientierten zu einer vorwiegend elektronischen Vorgangsbearbeitung gehört die Digitalisierung von (noch lange Zeit) eingehenden Papierdokumenten. Ist die Überführung von Papierdokumenten in die elektronische Form insbesondere im Handels- und Steuerrecht entsprechend den Grundsätzen ordnungsgemäßer Buchführung eine seit Jahrzehnten übliche Vorgehensweise, so besteht der Unterschied in dem einer beglaubigten Abschrift entsprechenden höheren Beweiswert, der auf diese Weise erreicht werden soll. Die Zielsetzung der Transformation ist, alle Dokumente, unabhängig von ihrem Schriftformerfordernis, *elektronisch zu beglaubigen* und diesen transformierten Dokumenten den gleichen Beweiswert wie dem jeweiligen Ursprungsdokument zukommen zu lassen. Die ursprüngliche Bedeutung der Beglaubigung besteht darin, das zumeist nur einmalig vorliegende *körperliche* Original für unterschiedliche Verwendungen zu vervielfältigen und diesen *Duplikaten* für den jeweiligen Beglaubigungszweck eine gleiche rechtliche Wirkung zukommen zu lassen. Das Original bleibt jedoch immer erhalten. Elektronisch signierte Dokumente können hingegen beliebig vervielfältigt werden. Bisherige Lösungen sehen lediglich die reine Digitalisierung dieser Dokumente vor; soweit Anforderungen an den Beweiswert solcher Dokumente bestehen, werden sie außerdem weiter im Originalzustand aufbewahrt. Das führt jedoch zu zusätzlichem Aufwand bei der Aktenhaltung. Durch die inzwischen in Kraft getretene Änderung des Verwaltungsverfahrensrechts wird in der öffentlichen Verwaltung erstmals die elektronische Beglaubigung von digitalisierten Papierdokumenten ermöglicht. Damit ist die Umsetzung eines elektronisch unterstützten einheitlichen Prozesses bei der Weiterverarbeitung im Rahmen von E-Government-Anwendungen möglich. Aufwändige Doppelimplementierungen werden vermieden. Auf der CeBIT 2003 hat das Informatikzentrum Niedersachsen bereits einen prototypischen Beglaubigungsarbeitsplatz vorgestellt.

## 5 Wie können große Organisationen eine kostengünstige Lösung für eine Vielzahl von Verfahren aufbauen?

Unverzichtbarer Bestandteil einer E-Government-Infrastruktur sind Systeme zur Unterstützung von elektronischen Akten. Die rechtlichen und technischen Rahmenbedingungen lassen inzwischen die Festlegung der elektronischen Akte als verbindliche führende Akte zu. In der öffentlichen Verwaltung wird für Schriftgut in der Regel eine dreistufige Aufbewahrungsform verwendet:

- Lebende Schriftgutablagen (digital: Kurzzeitspeicher):
  Die erste Stufe umfasst alle lebenden Vorgänge, das heißt alle Vorgänge, die sich noch in der Bearbeitung befinden. Technisch werden an dieser Stelle in der Praxis entweder Dokumentenmanagementsysteme (insbesondere nach dem DOMEA-Standard) oder bei bestehenden großen Fachanwendungen Eigenentwicklungen mit entsprechender Funktionalität eingesetzt.
- Altablage (digital: Langzeitspeicher):
  Nach Abschluss der Bearbeitung beziehungsweise eines Vorgangs erfolgt in der zweiten Stufe eine Aufbewahrung innerhalb von gesetzlichen (oder aus Gesetzen abgeleiteten) Fristen. Für eine Altablage wird technisch entweder das eingesetzte Dokumentenmanagementsystem oder ein gesondertes Archivsystem eingesetzt.
- Archivgut (digital: Archivspeicher):
  Nach Ablauf der gesetzlichen Aufbewahrungsfrist werden die Vorgänge oder Akten den Staatsarchiven zur archivischen Bewertung und gegebenenfalls dauerhaften Übernahme angeboten. Entscheidend für die Einstufung von Schriftgut als archivwürdig ist die Frage, ob es von bleibendem Wert ist für die Erfüllung öffentlicher Aufgaben, für die Sicherung berechtigter privater Interessen oder für die Forschung. Archivwürdige Vorgänge oder Akten werden daher als letzte Stufe ohne jede zeitliche Begrenzung (für die Ewigkeit) aufbewahrt. Als technisches System kommt an dieser Stelle nur ein Archivsystem in Frage.

Der Einsatz eines einheitlichen Dokumentenmanagementsystems zur Bildung von elektronischen Akten für *alle* Bereiche einer großen Organisation wie der niedersächsischen Landesverwaltung im Bereich der lebenden

Schriftgutablage wird wegen der Vielfalt der fachlichen und organisatorischen Anforderungen wohl nicht möglich sein. Angestrebt wird allerdings eine Begrenzung der eingesetzten Systeme auf eine möglichst geringe Anzahl. Die hohe Funktionalität aller zertifizierten DOMEA-Produkte rechtfertigt eine solche Begrenzung. Die Systeme unterscheiden sich im Wesentlichen lediglich durch ihre Systemarchitektur in Verbindung mit der Betriebsplattform und in der Benutzeroberfläche. In neueren Architekturen wird vorgeschlagen, dass Dokumentenmanagementfunktionen grundsätzlich nicht direkt in eine Anwendung implementiert werden sollen, sondern über definierte Schnittstellen von Dokumentenmanagementsystemen erledigt werden.

Anders als im Bereich der lebenden Schriftgutablagen kann im Bereich der Altablage und der Archivablage ein einheitliches technisches Verfahren zum Einsatz kommen. Auf der Basis der traditionellen Aufbewahrungsformen ist in dem niedersächsischen E-Government-Projekt „Langzeitarchivierung“ ein grundlegendes Speicherkonzept für die sichere Langzeitspeicherung von elektronisch signierten Dokumenten unter Erhaltung des Beweiswerts entwickelt worden. Das Konzept sieht die Aufbewahrung abgeschlossener Vorgänge in einem zentralen Langzeitspeicher vor. Dies hat den Vorteil, dass die aufwändigen Sicherungsmechanismen nicht in jedes Verfahren implementiert werden müssen. Nach Abschluss der Aufbewahrungsfristen können archivwürdige Dokumente ohne besonderen Aufwand in einen Archivspeicher übernommen werden. Er unterscheidet sich von dem Langzeitspeicher nur durch eine den Archiverfordernissen angepasste Ablage- und Retrievalstruktur. Außerdem werden die zur Rechtssicherheit erforderlichen elektronischen Signaturen durch einfache Informationen über den Signierenden ersetzt. Abbildung 4 zeigt die vorgeschlagene Architektur einer solchen Lösung.

Die erforderlichen konzeptionellen Arbeiten im Projekt sind weitgehend abgeschlossen. Zusammen mit einem Projektpartner beginnt jetzt die Umsetzung der entwickelten Konzepte. Dazu wird im Hochsicherheitsrechenzentrum nun auch eine physische Infrastruktur für den Langzeitspeicher und das zukünftige elektronische Staatsarchiv auf der technischen Basis des ArchiSig-Projekts aufgebaut. Das Zusammenspiel mit Fachanwendungen und Dokumentenmanagement wird anhand von Dokumenten aus dem niedersächsischen E-Government-Verfahren „Elektronischer Rechtsverkehr in

Familiensachen“ erprobt werden. Damit soll noch im kommenden Jahr der Beweis erbracht werden, dass eine dauerhafte rechtssichere Aufbewahrung von elektronisch signierten Dokumenten auch in der öffentlichen Verwaltung möglich ist. Es wird der Weg für den Aufbau einer Produktionsumgebung geöffnet und eines der letzten Hindernisse beim Übergang von der Papierbearbeitung zur elektronischen Bearbeitung aus dem Weg geräumt.

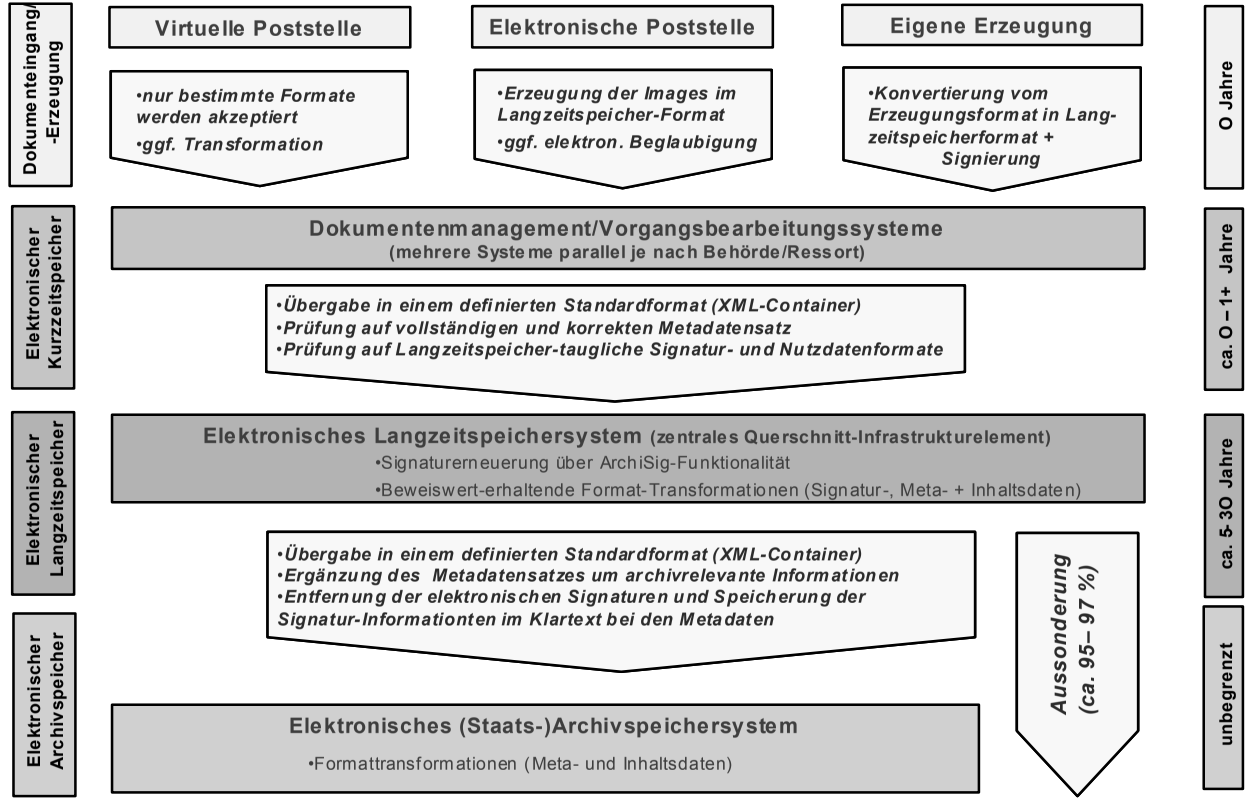
Dokumenteingang/ -Erzeugung
Virtuelle Poststelle
Elektronische Poststelle
Eigene Erzeugung
O Jahre
•nur bestimmte Formate werden akzeptiert
•ggf. Transformation
•Erzeugung der Images im Langzeitspeicher-Format
•ggf. elektron. Beglaubigung
•Konvertierung vom Erzeugungsformat in Langzeitspeicherformat + Signierung
Elektronischer Kurzzeitspeicher
Dokumentenmanagement/Vorgangsbearbeitungssysteme
(mehrere Systeme parallel je nach Behörde/Ressort)
ca. O – 1+ Jahre
•Übergabe in einem definierten Standardformat (XML-Container)
•Prüfung auf vollständigen und korrekten Metadatensatz
•Prüfung auf Langzeitspeicher-taugliche Signatur- und Nutzdatenformate
Elektronischer Langzeitspeicher
Elektronisches Langzeitspeichersystem (zentrales Querschnitt-Infrastrukturelement)
•Signaturerneuerung über ArchiSig-Funktionalität
•Beweiswert-erhaltende Format-Transformationen (Signatur-, Meta- + Inhaltsdaten)
ca. 5-30 Jahre
•Übergabe in einem definierten Standardformat (XML-Container)
•Ergänzung des Metadatensatzes um archivrelevante Informationen
•Entfernung der elektronischen Signaturen und Speicherung der Signatur-Informationten im Klartext bei den Metadaten
Aussonderung
(ca. 95– 97 %)
Elektronischer Archivspeicher
Elektronisches (Staats-)Archivspeichersystem
•Formattransformationen (Meta- und Inhaltsdaten)
unbegrenzt

Abbildung 4