Elektronische Signatur und Verschlüsselung in der öffentlichen Verwaltung. Eine Herausforderung für die Archivierung

von Gudrun Klee-Kruse

1. Einleitung

In den öffentlichen Verwaltungen spielt die Kommunikation über offene Computernetze – wie das Internet – eine immer wichtigere Rolle. So ist z. B. in zahlreichen Behörden die E-Mail Kommunikation sowohl untereinander als auch mit Bürgern und Unternehmen kaum noch wegzudenken. Durch die stetige Zunahme der Erzeugung elektronischer Daten und die elektroni-

sche Kommunikation von zum Teil hochsensiblen Daten, die über das Internet ausgetauscht werden, häufen sich allerdings auch die Fragen nach der Sicherheit der elektronischen Kommunikation. Lassen sich doch elektronische Daten während des Transportes zwischen Absender und Empfänger ohne große Probleme abfangen, lesen und ggf. verfälschen. Abhilfe bieten hier die Verschlüsselung von Daten und die elektronische Signatur. So sorgt die Verschlüsselung von Daten für die Gewährleistung der Geheimhaltung und Vertraulichkeit und die elektronische Signatur für die Sicherung vor der Datenverfälschung (Integrität), die Überprüfung des Nachrichtenursprungs (Authentizität) sowie den Beweis der Herkunft des Dokumentes (Verbindlichkeit).

2. Gesetzliche Vorgaben

Im Zivilrecht, im öffentlichen Recht wie auch im Prozessrecht sind in den vergangenen 3 Jahren auf Bundes- und Landesebene die rechtlichen Grundlagen geschaffen worden, um rechtsgültig einen elektronischen Rechts- und Geschäftsverkehr durchführen zu können. Im Regelfall kann die Schriftform durch elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur i. S. d. § 2 Nr. 3 Signaturgesetz (SigG) versehen sind, gleichwertig ersetzt werden.

2.1 Gesetzesänderungen

Signaturgesetz

Mit dem

- Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz– SigG) vom 16.05.2001 (BGBl I S. 876) und der
- Signaturverordnung vom 16.11.2001 (BGBl I S. 3074)

ist die Richtlinie 1999/93/EG vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen umgesetzt worden. Die Rechtsnormen definieren jedoch nur die verschiedenen Signaturarten, legen die Anforderungen an elektronische Signaturen fest und beschreiben, wie die Sicherheit und Unverfälschtheit von elektronischen Daten technisch und organisatorisch gewährleistet werden soll (Sicherheitsinfrastruktur). Sie regeln aber nicht die materiell- und verfahrensrechtlichen Folgen der Benutzung der elektronischen Signatur (Rechtswirkungen).

Gesetz zur Anpassung der Formvorschriften des Privatrechts

Im Bereich des Privatrechts ist mit dem am 1. August 2001 in Kraft getretenen

- Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr vom 13.07.2001 (BGBl I S. 1542)

die Grundlage zur Einführung der elektronischen Form als rechtlich gleichwertige Alternative zur eigenhändigen Unterschrift geschaffen worden. Nach dem neu eingefügten § 126 Abs. 3 BGB kann die gesetzlich vorgeschriebene Schriftform durch die elektronische Form gleichwertig und rechtswirksam ersetzt werden. Die elektronische Form ist gemäß § 126a Abs. 1 BGB gewahrt, wenn der Erklärende einem elektronischen Dokument seinen Namen hinzufügt und es mit einer qualifizierten elektronischen Signatur nach dem SigG versieht. Ausnahmen bestehen für besondere Willenserklärungen, in denen in den entsprechenden Vorschriften weiterhin ausdrücklich eine eigenhändige Unterschrift verlangt wird (z. B. Beendigung von Arbeitsverhältnissen; § 623 Halbsatz 2 BGB). Daneben ist für die gewillkürte Schriftform die Textform eingeführt worden, die weder den Einsatz einer qualifizierten noch einer fortgeschrittenen Signatur erfordert (§ 127 BGB).

Verwaltungsverfahrensgesetz

Im öffentlich rechtlichen Verwaltungsverfahren wurde der rechtliche Rahmen für elektronische Kommunikation auf Bundesebene mit dem 3. Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften und auf Landesebene durch entsprechende Änderungen der jeweiligen Verwaltungsverfahrensgesetze der Länder geschaffen. Nach dem zwischen Bund und Ländern abgestimmten Gesetz können Bürger und Verwaltung grundsätzlich in allen Fachgebieten und jeder Verfahrensart elektronische Kommunikationsformen gleichberechtigt neben der Schriftform und der mündlichen Form verwenden. In Generalklauseln (z. B. § 3a Abs. 2 Satz 1 VwVfG-Entwurf) wird in bewusster Anlehnung an § 126a BGB geregelt, dass ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur verbunden wird, den durch Rechtsnormen angeordneten Schriftformerfordernissen gleichgestellt ist. Diese Generalklausel erfasst nicht nur die Schriftformerfordernisse in den Verwaltungsverfahrensgesetzen, sondern grundsätzlich das gesamte besondere Verwaltungsrecht. Ausnahmen bedürfen einer ausdrücklichen Regelung. Der elektronische Verwaltungsakt wurde als neuer Typ eingeführt (§ 37 Abs. 2 VwVfG). Bei zahlreichen Verwaltungsakten mit besonderer Bedeutung wird die dauerhafte Überprüfbarkeit der qualifizierten elektronischen Signatur verlangt.

Nach dem derzeitigen Stand der Technik erfordert dies qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung i. S. d. § 15 SigG, deren Zertifikate mindestens 30 Jahre überprüfbar sein müssen.

Demgegenüber ist für die Kommunikation des Bürgers mit der Verwaltung bei förmlichen Verfahrenshandlungen die qualifizierte elektronische Signatur ohne Anbieterakkreditierung (Class 3) ausreichend. Schließlich sind im Bereich des formfreien Verwaltungshandelns weiterhin einfache elektronische Handlungsformen möglich, die rechtlich keiner elektronischen Signatur bedürfen.

Gesetz zur Reform des Verfahrens bei Zustellungen im gerichtlichen Verfahren

Mit dem

- Gesetz zur Reform des Verfahrens bei Zustellungen im gerichtlichen Verfahren (ZustRG) vom 25.06.2001 (BGBl I S. 1206)

und dem o. g. Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr hat der Gesetzgeber erste Schritte zur Öffnung der Justiz für den elektronischen Rechtsverkehr unternommen.

Die Gesetze enthalten die rechtlichen Grundlagen dafür, dass (vorbereitende und bestimmende) Schriftsätze alternativ und rechtsgültig in Form von elektronischen Dokumenten bei Gericht eingereicht werden und elektronische Zustellungen vom Gericht erfolgen können. Nach den Ermächtigungsgrundlagen sollen solche elektronischen Dokumente mit einer qualifizierten elektronischen Signatur versehen werden. Der Zeitpunkt, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können, wird durch Rechtsverordnungen bestimmt.

Für den Bundesgerichtshof ist am 30.11.2001 die Verordnung über den elektronischen Rechtsverkehr beim BGH (BGBl I S. 3225) in Kraft getreten. Seitdem erprobt das oberste Zivilgericht in einem ausgewählten Testsenat den elektronischen Rechtsverkehr. Daneben erarbeitet derzeit eine Bund-Länder-Arbeitsgruppe »Elektronischer Rechtsverkehr« unter dem Vorsitz des Bayerischen Staatsministeriums der Justiz organisatorisch-technische Leitlinien für den elektronischen Rechtsverkehr. Auf der Grundlage dieser Leitlinien sollen koordinierte Länderverordnungen mit dem Ziel erstellt werden, die Zugangsvoraussetzungen und sonstigen Rahmenbedingungen für den elektronischen Rechtsverkehr in den Ländern gleich zu gestalten.

Zivilprozessordnung

Der ebenfalls mit dem Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr eingefügte § 292a der Zivilprozessordnung (ZPO) führt einen Anscheinsbeweis zu Gunsten der elektronischen Form (s. § 126a BGB) ein. Der Anscheinsbeweis kann nur durch Tatsachen erschüttert werden, die es ernsthaft als möglich erscheinen lassen, dass die Erklärung nicht mit dem Willen des Signaturschlüsselinhabers abgegeben worden sind.

2.2 Die Bedeutung des Datenschutzes für die elektronische Kommunikation

Spezielle Vorschriften für den Einsatz von Verschlüsselungsmechanismen bei der Übermittlung von elektronischen Daten sind z. B. im Verwaltungsverfahrensgesetz (VwVfG) des Landes NRW nicht enthalten. In der Begründung zu § 30 VwVfG wird jedoch ausgeführt, dass die notwendigen Sicherheitsvorkehrungen für die elektronische Datenübertragung (Einsatz von Verschlüsselungstechniken) zu treffen sind. Weitergehende Ausführungen fehlen, so dass im Kontext die Bestimmungen des Datenschutzes einzubeziehen sind.

Das Landesdatenschutzgesetz NRW z. B. führt in diesem Zusammenhang aus, dass der Absender einer Information ein Recht darauf hat, dass die erhobenen Daten nur für den Zweck verwendet werden, der Grundlage für die Erhebung der Daten war (§ 4 Landesdatenschutzgesetz NRW). Dies setzt Vertraulichkeit der Daten bei der Übertragung voraus. Der Begriff der Vertraulichkeit steht für die Gewährleistung, dass Daten und Informationen vor Unbefugten geheim bleiben. Im Fall der konventionellen Kommunikation wird Vertraulichkeit durch verschlossene Briefe, persönliche Gespräche etc. erreicht. Dabei kann es zu Abstufungen der Ausprägung kommen. Beispielsweise ist ein Gespräch am Schalter weniger vertraulich als ein Gespräch im Büro des Behördenmitarbeiters.

Werden Informationen elektronisch übertragen, ist die Wahrscheinlichkeit allerdings sehr groß, dass die Informationen Unbefugten zur Kenntnis gelangen, von diesen manipuliert oder durch technische Fehler verändert werden. Aus diesem Grund ist es z. B. in Behörden nicht gestattet, vertrauliche Daten und Daten mit Personenbezug ungeschützt elektronisch zu verschicken.

Die Empfehlung der Landesdatenschutzbeauftragten aller Bundesländer lautet daher: »Personenbezogene und vertrauliche Daten sollten grundsätzlich bei der Übertragung über öffentliche Leitungen (Internet) verschlüsselt werden«. Da häufig für den Einzelnen nicht abschätzbar ist, wie sensitiv die zu übertragenden Daten sind, sollte – so die Datenschutzbeauftragten – die **Verschlüsselung als Grundschutzmaßnahme** insbesondere bei Datenübertragungen über das Internet eingesetzt werden.

3. Elektronische Signaturen

3.1 Grundlagen zum Verfahren des elektronischen Signierens

Die drei wesentlichen Ziele, die man mit dem Einsatz elektronischer Signaturen erreichen will, sind die Gewissheit über die Echtheit und Unverfälschtheit des signierten Dokumentes sowie die Sicherstellung der Identität des Unterzeichners. Man spricht in diesem Zusammenhang von den drei Sicherheitszielen der elektronischen Signatur:

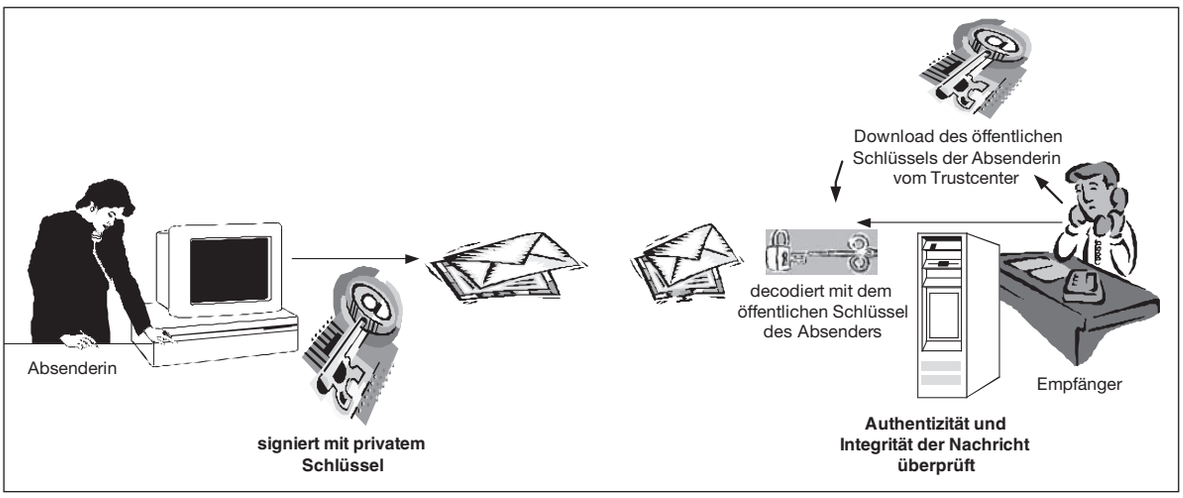
- **Integrität (Daten können nicht unerkannt gefälscht werden)**
- **Verbindlichkeit (Beweis der Herkunft)**
- **Authentizität (Möglichkeit des Überprüfens des Nachrichtenursprungs)**

Was aber ist nun eine elektronische Signatur?

Der Begriff elektronische Signatur verdankt seinen Namen der Analogie zur eigenhändigen Unterschrift und stellt im Sinne des Signaturgesetztes eine Art elektronisches Siegel zu elektronischen Daten dar, dass den Absender und die Unverfälschtheit der Daten erkennen lässt.

Elektronische Signaturen basieren auf dem Verfahren der asymetrischen Kryptographie. Hierbei kommen korrespondierende Schlüsselpaare bestehend aus einem **privaten** und einem **öffentlichen** Schlüssel zum Einsatz. Der private Schlüssel ist ein geheimer Schlüssel, der individuell einer Person zugeordnet ist und im Regelfall auf einer Chipkarte abgespeichert wird. Zu dem privaten Schlüssel gehört ein öffentlicher Schlüssel, der wie der Name schon sagt öffentlich bekannt gemacht wird. Der private und der öffentliche Schlüssel bilden zusammen das Schlüsselpaar, dass benötigt wird, um den Vorgang des Signierens durchzuführen. Den privaten Schlüssel nutzt der Signierende zur Signaturerzeugung, während der öffentliche Schlüssel dem Empfänger des Dokumentes oder der E-Mail zur Signaturprüfung dient.

Bei der Erzeugung einer elektronischen Signatur wird aus dem elektronischen Dokument mit Hilfe ei-



Vorgang des Signierens

ner Hashfunktion[1] eine eindeutige Prüfsumme (Hashwert) fester Länge errechnet. Diese Prüfsumme wird nun mit dem privaten Schlüssel des Unterzeichners verschlüsselt und als elektronische Signatur an das Dokument angehängt. Die elektronische Signatur ist also die Verschlüsselung des Hashwertes eines Dokumentes und nicht des Dokumentes selbst. Zu jedem Dokument gibt es nur einen Hashwert. Sobald nur ein Zeichen oder eine Ziffer des Dokumentes verändert wird, ist der Hashwert des Dokumentes ein völlig anderer.

Der verschlüsselte Hashwert des Dokumentes wird an den Empfänger geschickt. Zur Überprüfung der Integrität, der Verbindlichkeit und Authentizität des signierten elektronischen Dokumentes wird auf Seiten des Empfängers erneut die Prüfsumme des Dokumentes mit Hilfe der Hashfunktion gebildet. Dann wird mit dem öffentlichen Schlüssel des Absenders der Hashwert des übersandten Dokumentes entschlüsselt, um die beiden Prüfsummen miteinander vergleichen zu können. Sind beide Prüfsummen gleich, so ist die Integrität des Dokumentes bewiesen.

Vorgang des Signierens

Wie aber wird sichergestellt, dass der öffentliche Schlüssel, den der Empfänger eines Dokumentes zur Signaturprüfung verwendet, tatsächlich zu dem privaten Schlüssel des Absenders gehört? Wie also wird die Verbindlichkeit der Signatur sichergestellt?

Die Zuordnung von Schlüsseln bzw. Schlüsselpaaren zu Personen erfolgt über Zertifikate, die den Schlüsseln beigefügt werden. Die Ausstellung der Zertifikate und damit die Gewährleistung der richtigen öffentlichen Schlüsseln zu den privaten Schlüsseln wird durch eine vertrauenswürdige Instanz vorgenommen, die sogenannte Zertifizierungsstelle, die in Deutschland häufig auch als Trustcenter bezeichnet wird. Bei jeder Signaturprüfung besorgt sich der Empfänger einer signierten Nachricht über das Trustcenter das Zertifikat des Absenders mit dem jeweiligen öffentlichen Schlüssel. Ferner führen die Trustcenter sogenannte Sperrlisten zur Überprüfung der Gültigkeit des Zertifikates. Das Herunterladen des öffentlichen Schlüssels sowie die Überprüfung der Sperrlisten beim Trustcenter erfolgt i. d. R. automatisiert.

3.2 Funktionsweise der Verschlüsselung

Sofern neben den drei oben genannten Sicherheitszielen: Authentizität, Integrität und Verbindlichkeit der Daten bei der Datenübertragung gewährleistet werden soll, dass die Informationen auf dem Weg zum Empfänger geheimgehalten werden, kommt der Sicherheitsmechanismus der **Verschlüsselung** zum Tragen.

Bei der Verschlüsselung eines elektronischen Dokumentes kommen – wie bei der elektronischen Signatur – kryptographische Techniken zum Einsatz, die aus zwei Komponenten bestehen: Einem privaten und einem öffentlichen Schlüssel. Der private Schlüssel wird auch hier auf der Chipkarte gespeichert, der öffentliche Schlüssel wird öffentlich bekannt gegeben, d. h. anderen Internetnutzern zugänglich gemacht. Dies kann über die Homepage einer Behörde, eines Unternehmens etc. geschehen oder aber der öffentliche Schlüssel wird von einem Trustcenter bereitgestellt.

Für den Vorgang des Verschlüsselns wird der öffentliche Schlüssel des Empfängers einer Nachricht eingesetzt, um beim Versand durch den Absender Daten verschlüsseln zu können. Dafür muss der Absender einer Nachricht zunächst den öffentlichen Schlüssel des Empfängers von dessen Homepage herunterladen oder den Schlüssel beim Trustcenter anfordern. Da der private Schlüssel des Empfängers die einzige und notwendige Ergänzung zu dem zum Verschlüsseln verwendeten öffentlichen Schlüssel darstellt, kann nur mit dem entsprechenden privaten Schlüssel des Empfängers der verschlüsselten Nachricht diese entschlüsselt werden.

3.3 Unterscheidung von elektronischen Signaturen

Das Signaturgesetz unterscheidet zwischen drei unterschiedlichen Sicherheitsniveaus für elektronische Signaturen:

- Einfache Signaturen
- Fortgeschrittene Signaturen
- Qualifizierte Signaturen
- sowie qualifizierte Signaturen eines akkreditierten Zertifizierungsanbieters

1 Ein Hashwert ist eine durch eine mathematische Funktion errechnete Kurzfassung von elektronischen Daten.

Die (einfache) elektronische Signatur / Class 1 (z. B. eingescannte Unterschrift) ist nicht zweifelsfrei einer Person zuzuordnen. Sie erfüllt keine besonderen Sicherheitsanforderungen und hat daher wenig Beweiswert. Sie kommt nur für formfreie Vorgänge in Betracht.

Fortgeschrittene Signaturen / Class 2 genügen bereits erhöhten Anforderungen, lassen insbesondere eine Authentifizierung des Signaturschlüssel-Inhabers und die Überprüfung der Integrität der übermittelten Daten zu. Sie ersetzen jedoch weder im Zivil- noch im öffentlichen Recht eine etwa vorgeschriebene Schriftform. Fortgeschrittene Signaturen können sowohl von akkreditierten Trustcentern als auch von genehmigungsfreien Trustcentern bezogen werden. Es besteht aber auch die Möglichkeit, eigene Trustcenterfunktionalitäten aufzubauen.

Qualifizierte elektronische Signaturen (ohne Anbieterakkreditierung) / Class 3 erfüllen die Voraussetzungen der fortgeschrittenen Signaturen und werden mit einer sicheren Signaturerstellungseinheit erzeugt. Sie werden ausschließlich von Zertifizierungsdiensteanbietern (Trust-Centern) ausgestellt, deren Betrieb zwar genehmigungsfrei ist, die jedoch gesetzlich geforderte Voraussetzungen erfüllen müssen. Die Aufnahme des Trust-Center-Betriebs ist der Regulierungsbehörde für Post und Telekommunikation (RegTP) anzuzeigen. Die qualifizierte elektronische Signatur erfüllt hohe Sicherheitskriterien, ist für die Authentifizierung geeignet und bietet ein hohes Maß an Beweiskraft. Die Zertifikate müssen für den Gültigkeitszeitraum (3–5 Jahre) sowie fünf weitere Jahre aufbewahrt werden. Qualifizierte elektronische Signaturen können sowohl im Zivilrecht als auch im öffentlichen Recht die Schriftform ersetzen.

Qualifizierte elektronische Signaturen mit Anbieterakkreditierung / Class 4 erfüllen die Voraussetzungen der qualifizierten elektronischen Signaturen und entfalten grundsätzlich die gleichen Rechtswirkungen. Darüber hinaus garantieren die Zertifizierungsdiensteanbieter jedoch eine nachgewiesene organisatorische und technische Sicherheit. Vor Aufnahme des Betriebs erfolgt eine umfassende Sicherheitsüberprüfung, die Anbieter erhalten anschließend ein »Gütesiegel«. Ein weiterer Unterschied liegt in der langfristigen Überprüfbarkeit der Zertifikate (mindestens 30 Jahre). Zusätzliche Anforderungen wie z. B. die dauerhafte Überprüfbarkeit können im öffentlichen Recht für einzelne, genau bestimmte Vorgänge als Voraussetzung festgelegt werden. Eine generelle Festlegung dieser Signaturstufe ist jedoch nicht möglich. Im Zivilrecht kann diese Stufe überhaupt nicht gefordert werden.

4. Langzeitarchivierung von elektronisch signierten und verschlüsselten Dokumenten

Im Gegensatz zu Papierdokumenten können elektronisch signierte Dokumente im Laufe der Zeit an Beweiswert verlieren. Die Ursachen hierfür sind, dass

a) die verwendeten kryptographischen Verfahren aufgrund der technischen Entwicklung nicht mehr sicher genug sind
b) die für die Überprüfung der elektronischen Signatur notwendigen Informationen zu den zugrundeliegenden Zertifikaten und deren eventueller Sperrung nicht über einen langen Zeitraum verfügbar sind.

Nur für die elektronischen Signaturen der akkreditierten Trustcenter beträgt die Aufbewahrungsfrist 30 Jahre, so dass eine längerfristige Verfügbarkeit der zur Zertifikatsprüfung erforderlichen Informationen für diesen Zeitraum gegeben ist. Über den Zeitraum von 30 Jahren hinaus jedoch sowie für die übrigen elektronischen Signaturen gilt, dass eine beweiskräftige Archivierung nicht unbedingt gewährleistet wird bzw. werden kann. Vielmehr sind ergänzende Maßnahmen erforderlich, um den Beweiswert elektronisch signierter Dokumente zu erhalten.

Dies bedeutet, dass alle zur Verifizierung (Überprüfung) elektronischer Dokumente erforderlichen Verifikationsdaten (Zertifikate, Sperrlisten, Zertifikatsstatusabfragen beim Trustcenter) sowie ggf. die Zertifikate für die Entschlüsselung des Dokumentes vor der Archivierung beschafft werden und in einer beweisfähigen Form gespeichert sein müssen, um den späteren Datenaustausch sowie die Migration von Anwendungssystemen einschließlich der gespeicherten Dokumente und Verifikationsdaten zu ermöglichen.

Insgesamt liegen bislang nur wenig Erfahrungen zur langfristigen Archivierung elektronischer signierter und ggf. noch verschlüsselter Unterlagen vor. Konzepte elektronisch signierte Daten über einen Zeitraum von 30 Jahren hinaus beweiskräftig, datenschutzkonform und kostengünstig zu archivieren, werden derzeit entwickelt bzw. erprobt[2]. Bis zur breiten Anwendbarkeit solcher Konzepte gilt es jedoch schon heute zu beachten, dass sowohl die Zertifikate für die Ver- und Entschlüsselung eines elektronischen Dokumentes als auch die gesamten Verifikationsdaten für die elektronischen Signaturen so vorgehalten und gespeichert sein müssen, dass sie über die relativ kurze Verfügbarkeit der Zertifikate (3–5 Jahre) hinaus verfügbar sind. Die Anforderungen an die »Archivierung« der erforderlichen Verifikations- und Entschlüsselungsdaten stellen sich bereits lange bevor die »Langzeitsicherung« eines Dokumentes zur Aufgabe der Archivarin und des Archivaren wird.

2 Vgl. hierzu das Projekt ArchiSig zur Langzeitsicherung elektronisch signierter Dokumente. Dieses vom Bundesministerium für Wirtschaft und Technologie geförderte Verbundprojekt hat es sich zum Ziel gesetzt, technische Lösungen und Konzepte für die Langzeitarchivierung elektronisch signierter Dokumente für die öffentliche Verwaltung und das Gesundheitswesen zu erarbeiten.