Vertrauenswürdige elektronische Langzeitspeicherung

Version: 1.0

Status: freigegeben

Dokumenteninformationen

Thema/Bezeichnung

Vertrauenswürdige elektronische Langzeitspeicherung

Sächsische Anstalt für kommunale Datenverarbeitung

Version	1.0
Status	freigegeben
Datum der letzten Änderung	07.07.2010
Autoren, Ansprechpartner	Horst Pohle, SAKD

Inhalt

1 Einleitung

Die Rahmenkonzeption zur IT-Umsetzung der EU-DLR in den Kommunalverwaltungen im Freistaat Sachsen behandelte die Themen:

- Informationsbereitstellung für den Verwaltungskunden und den Einheitlichen Ansprechpartner (EA),
- Rechtssichere Kommunikation mit dem Verwaltungskunden und EA und
- Bereitstellung von Online-Formularen für den Verwaltungskunden.

In den nun folgenden Ausführungen wird auf die rechtssichere bzw. vertrauenswürdige Ablage der kommunizierten elektronischen Dokumente eingegangen.

Hinsichtlich der Ablage ist dabei konsequent zwischen der Langzeitspeicherung und der Archivierung der Dokumente zu unterscheiden. Für Dokumente der öffentlichen Verwaltung gelten gesetzlich festgelegte Aufbewahrungsfristen. Innerhalb dieser Fristen sind die Dokumente in der Behörde für den direkten Zugriff aufzubewahren. Hierfür hat sich im Sprachgebrauch auch der Begriff der *elektronischen Langzeitspeicherung* eingebürgert, um den Unterschied zur kurzzeitigen (operativen) Speicherung bzw. zum Backup hervorzuheben. Bei der Langzeitspeicherung wird aus informationstechnischer Sicht ein Zeithorizont von 10 bis 30 Jahren betrachtet, man spricht auch von einer *zeitlich befristeten Aufbewahrung.*

Unterlagen der öffentlichen Verwaltung, welche für die Zwecke der Behörde nicht mehr benötigt werden, sind dem zuständigen Archiv anzubieten. Die als archivwürdig befundenen Dokumente sind dann im Archiv auf unbegrenzte Zeit zu verwahren. Unter *elektronischer Archivierung* wird daher allgemein die dauerhafte und unveränderbare Aufbewahrung (Speicherung) von elektronischen Dokumenten und Daten verstanden.

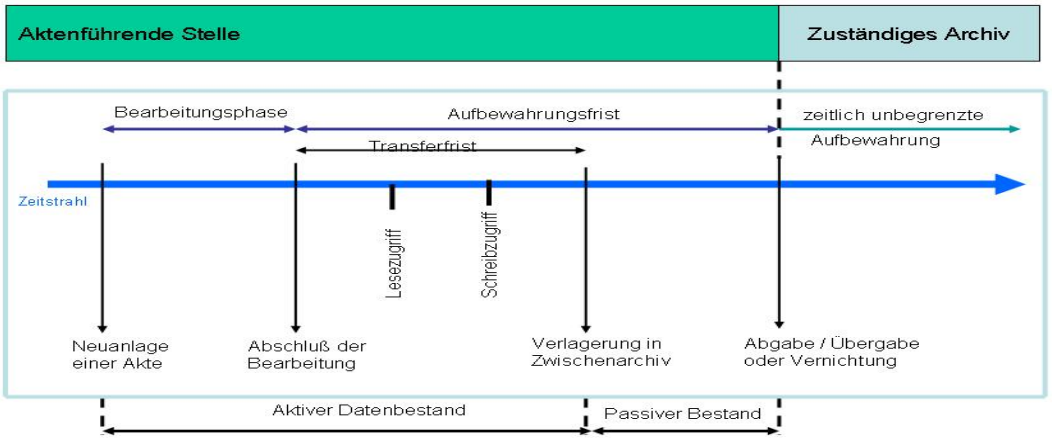

Abb: Lebenszyklus eines Dokuments

Das Ziel einer auf lange Zeiträume angelegten vertrauenswürdigen Ablage elektronischer Unterlagen ist die dauerhafte, rechts- und revisionssichere Speicherung digitaler Dokumente und Daten sowie zugehöriger Metainformationen. Für rechtlich bedeutsame Dokumente und Daten sind dabei zusätzlich nachprüfbare Belege über den Aussteller (**Authentizität**) sowie die Unversehrtheit (**Integrität**) der aufbewahrten Dokumente und Daten dauerhaft und entsprechend der rechtlichen Anforderungen vorzuhalten.

IT-Verfahren, die für eine Schriftgutverwaltung bzw. Dokumentenverwaltung und deren Langzeitspeicherung eingesetzt werden, müssen insoweit den Anforderungen an eine ordnungsgemäße Schriftgut- bzw. Dokumentenverwaltung genügen. Systemtechnische Lösungen für die Aufbewahrung von Dokumenten im Rahmen geltender Aufbewahrungsfristen sind in Form von Dokumentenmanagementsystemen (DMS) am Markt verfügbar.

Die nachfolgenden Ausführungen beziehen sich auf die Nutzung eines Langzeitspeichersystems in Behörden während der Aufbewahrungsfrist des Schriftgutes unter Wahrung der Rechtssicherheit und der Revisionssicherheit.

2 Begriffsdefinitionen

Rechtssichere elektronische Langzeitspeicherung bedeutet, dass das elektronische Speichersystem den beweisrechtlichen Wert der in ihm aufbewahrten elektronischen Informationen für die Dauer des Aufbewahrungszeitraumes sicherstellt und so die mit der Aufbewahrung elektronischer Unterlagen bezweckten Rechtsfolgen für die Dauer der gesetzlich vorgeschriebenen Aufbewahrungszeiträume gewährleistet.

Revisionssichere elektronische Langzeitspeicher sind elektronische Speichersysteme, die nach Vorgabe des Handelsgesetzbuches, der Abgabenordnung und der Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme elektronische Daten und Dokumente sicher, unveränderbar, vollständig, ordnungsgemäß, verlustfrei reproduzierbar und datenbankgestützt recherchierbar vorhalten.

Vertrauenswürdige elektronische Langzeitspeicherung ist die langfristige, rechts- und revisionssichere elektronische Speicherung von aufbewahrungspflichtigen Dokumenten und Daten einschließlich der zugehörigen Verwaltungsdaten (Metadaten) auf maschinenlesbaren Datenträgern zur Erfüllung der gesetzlichen Aufbewahrungspflichten.

Elektronische Signatur

Unter einer elektronischen Signatur versteht man Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder mit ihnen verknüpft sind und die zur Authentifizierung des Kommunikationspartners und dem Nachweis der Integrität der Daten im elektronischen Rechts- und Geschäftsverkehr dienen.

Eine elektronische Signatur bezieht sich immer auf ein elektronisches Dokument. Sie kann in dem Dokument selbst enthalten sein oder als zusätzliche Datei erstellt werden. Das Signaturgesetz (SigG) unterscheidet zwischen folgenden Typen von elektronischen Signaturen:

- **einfache elektronische Signaturen** (§ 2 Nr. 1 SigG)
  Einfache elektronische Signaturen dienen dazu, den Urheber einer elektronischen Nachricht zu kennzeichnen, z. B. durch das Abspeichern einer eingescannten Unterschrift. Für einfache elektronische Signaturen sind keine Anforderungen bezüglich ihrer Sicherheit oder Fälschungssicherheit definiert, so dass diese Signaturen nur einen sehr geringen Beweiswert haben. Sie erfüllt keine besonderen Sicherheitsanforderungen, ihr Beweiswert ist daher gering. Vor allem kann mit dieser Form eine Signatur

nicht eindeutig einer Person zugeordnet werden, daher eignet sie sich lediglich für formfreie Verträge.

- **fortgeschrittene elektronische Signaturen** (§ 2 Nr.2 SigG)
  Für fortgeschrittene elektronische Signaturen gelten höhere Anforderungen. Sie müssen eine Manipulation der Daten erkennbar machen, sich eindeutig einer natürlichen Person zuordnen lassen, die Identifizierung dieser Person erlauben und es ermöglichen, dass nur diese Person die erforderlichen Mittel zur Signaturerzeugung unter ihrer alleinigen Kontrolle halten kann. Insofern verfügen fortgeschrittene elektronische Signaturen grundsätzlich über einen etwas höheren Beweiswert. Die tatsächliche Sicherheit einer fortgeschrittenen elektronischen Signatur hängt jedoch von den eingesetzten Signaturverfahren, den verwendeten Software- und Hardwarekomponenten und nicht zuletzt von der Sorgfalt der Anwender bei der Signaturerstellung ab. Im Streitfall muss der Anwender daher im Zweifel beweisen, dass die Signatur tatsächlich in diesem Sinne sicher erzeugt wurde.

- **qualifizierte elektronische Signaturen** (§ 2 Nr.3 SigG)
  Bei dieser höchsten Sicherheitsstufe der elektronischen Signatur wird die Signatur ihrem Urheber über ein qualifiziertes Zertifikat (§ 2 Nr. 7 SigG) zugeordnet. Durch das qualifizierte Zertifikat, das von einem vertrauenswürdigen Zertifizierungsdiensteanbieter (§ 2 Nr. 8 SigG) (ZDA) signiert wird, wird die Zusammengehörigkeit zwischen dem öffentlich bekannten Signaturprüfschlüssel, der zur Prüfung der Signatur verwendet wird, und der Identität des Signaturschlüsselinhabers belegt. Der Zertifizierungsdiensteanbieter garantiert, dass die Angaben im qualifizierten Zertifikat und die Auskünfte seiner Verzeichnis- und Zeitstempeldienste korrekt sind und er die Anforderungen gemäß Signaturgesetz und Signaturverordnung erfüllt. Dazu gehört, dass der ZDA die sensiblen Zertifizierungsdienste in einer besonders geschützten Umgebung betreibt (Trust Center). Außerdem klärt der ZDA den Anwender über seine Sorgfaltspflichten im Umgang mit der Signatur auf. Zertifizierungsdiensteanbieter unterliegen der Aufsicht durch die Bundesnetzagentur (BNetzA) und müssen dort im Rahmen ihrer Betriebsaufnahme und Betriebsanzeige Nachweise, Belege und Erklärungen einschließlich eines Sicherheitskonzepts einreichen, die die Erfüllung der gesetzlichen Anforderungen gemäß Signaturgesetz und Signaturverordnung dokumentieren.
  Qualifizierte elektronische Signaturen sind wegen ihres hohen Sicherheitsniveaus in der Regel der handschriftlichen Unterschrift gleichgestellt und können grundsätzlich im Rechtsverkehr ebenso wie diese eingesetzt werden.
  Die qualifizierte elektronische Signatur wird mit einer sicheren Signaturerstellungseinheit (SSEE) erzeugt (zum Beispiel mit dem Chip einer Chipkarte).

3 Allgemeine Anforderungen an ein vertrauenswürdiges elektronisches Langzeitspeichersystem

Elektronische Langzeitspeichersysteme sichern für die Dauer der gesetzlich festgelegten Aufbewahrungspflicht den beweisrechtlichen Wert elektronisch aufbewahrter Informationen zum Nachweis eines ordnungsgemäßen Handelns sowie der Einhaltung der gesetzlichen Vorschriften und Regelungen. Anforderungen an die Dokumentation und Aufbewahrung sind aus den für den jeweiligen Sachbereich geltenden Normen und Vorschriften abzuleiten. Derzeit existiert keine einheitliche EU-Norm, welche die speziellen Anforderungen für die langfristige Aufbewahrung elektronischer Dokumente und Daten formuliert.

In der Bundesrepublik Deutschland normieren im Wesentlichen das Verwaltungsverfahrensgesetz (VwVfG), Signaturgesetz (SigG) und die Signaturverordnung (SigV) die Voraussetzungen und Anforderungen an die beweisrechtliche Anerkennung und den Erhalt des beweisrechtlichen Wertes elektronischer Unterlagen.

3.1 Rechtliche Rahmenbedingungen

3.1.1 Datenschutzrechtliche Regelungen

Bei der Speicherung personenbezogener Informationen sind insbesondere die datenschutzrechtlichen Regelungen des Bundesdatenschutzgesetzes und des sächsischen Datenschutzgesetzes zu beachten. Für eine langfristige vertrauenswürdige Aufbewahrung personenbezogener Daten ist durch organisatorische und technische Maßnahmen sicher zu stellen, dass

- nichtautorisierte Zugriffe auf schützenswerte Daten zuverlässig verhindert werden,
- Informationen und Daten weder vorsätzlich noch fahrlässig unbemerkt und in unzulässiger Weise manipuliert werden können,
- Veränderungen an Daten und Informationen protokolliert werden und
- ein unwiederbringlicher Verlust an diesen ausgeschlossen werden kann.

Das umfasst nicht nur technische, sondern auch organisatorische und gegebenenfalls bauliche Maßnahmen.

3.1.2 Signaturrechtliche Reglungen

Elektronische Signatur

Elektronische Daten und Dokumente könne ohne Hinterlassen von Spuren verändert bzw. manipuliert werden. Daher kann aus einem elektronischen Dokument alleine weder zuverlässig auf seinen tatsächlichen Aussteller (Authentizität) noch auf den tatsächlichen vom Aussteller beabsichtigten Inhalt (Integrität) geschlossen werden.

Elektronische Signaturen sind nach heutigem Kenntnisstand das am besten geeignete Sicherungsmittel, um die Integrität und Authentizität von elektronischen Daten und Dokumenten zu gewährleisten. Nach § 371a Abs.1 und Abs.2 sowie § 437 Abs.1 der Zivilprozessordnung (ZPO) wird von der Vorlage einer qualifizierten elektronischen Signatur auf den Anschein der Echtheit des Dokumentes geschlossen, sofern die Signatur dem Dokument zweifelsfrei zugerechnet werden kann. Der Anschein bzw. die Vermutung der Echtheit signierter elektronischer Dokumente bezieht sich dabei sowohl auf die Zurechnung des Dokuments zu dem Signaturschlüssel-Inhaber als auch auf die in dem Dokument niedergelegten Tatsachen oder Informationen. Voraussetzung für die Bestimmung des Beweiswertes eines elektronisch signierten Dokumentes ist die Durchführung einer Signaturprüfung.

Für den langfristigen Nachweis der Authentizität signierter Daten ist daher wesentlich, dass die Existenz des Nutzerzertifikats sowie seine Gültigkeit zum Signaturerstellungszeitpunkt nachweisbar bleiben.

Zeitstempel

Zeitstempel sind eine nachprüfbare Bestätigung, dass bestimmte Daten zu einem bestimmten Zeitpunkt existiert haben. In einer elektronischen Signatur ist normalerweise auch ein

Signaturzeitpunkt enthalten. Als Zeitangabe wird durch die Signatursoftware überwiegend die lokale Systemzeit verwendet. Diese Zeitangabe kann jedoch durch den Benutzer beliebig eingestellt werden und gilt deshalb nicht als vertrauenswürdig. Ein höheres Maß an Vertrauenswürdigkeit wird durch Zeitstempel erreicht, die von einer vertrauenswürdigen Instanz ausgestellt werden. Nach dem Signaturgesetz werden Zeitstempel als qualifizierte Zeitstempel bezeichnet, wenn sie von Dienstanbietern erzeugt werden, welche die Anforderungen des Signaturgesetzes und der Signaturverordnung erfüllen. Elektronische Signaturen in der Kombination mit qualifizierten Zeitstempeln entsprechen Beglaubigungen durch vertrauenswürdige Dritte.

Für elektronische Signaturen, basierend auf einem qualifizierten Zertifikat, sind für den schlüssigen und nachvollziehbaren Nachweis der Existenz und der Gültigkeit des Zertifikates zum Signaturerstellungszeitpunkt die Vorlage und technische Verifikation folgender Daten erforderlich

- das Nutzerzertifikat und ggf. Attributzertifikat (z. B. zu berufsbezogenen Angaben) mit Zertifikatskette bis zum Wurzelzertifikat,
- eine OCSP (Online Certificate Status Protocol) – Auskunft des Zertifizierungsdiensteanbieters über die Existenz und Gültigkeit des Zertifikats bis zum Wurzelzertifikat,
- ein qualifizierter Zeitstempel bezogen auf die Signatur mit Zertifikatskette bis zum Wurzelzertifikat.

Signaturerneuerung

Eine weitere erforderliche Maßnahme zur Sicherung der langfristigen Prüfbarkeit der Integrität signierter Daten ist die Signaturerneuerung nach § 17 SigV. Daten mit einer qualifizierten elektronischen Signatur sind neu zu signieren, wenn sie für längere Zeit benötigt werden, als der Signaturalgorithmus als geeignet (technisch sicher) beurteilt werden kann.

In diesem Fall sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen (zur Hashwertbildung, Verfahren zur Signaturschlüsselbildung) neu zu signieren. Verifikationsdaten enthalten ebenfalls elektronische Signaturen und unterliegen deshalb ebenso dem Erfordernis der Neusignierung nach § 17 SigV. Erst durch die Neusignierung kann die Unversehrtheit und damit die Echtheit eines Zertifikates, einer Gültigkeitsabfrage oder eines Zeitstempels langfristig überprüft werden.

Die Neusignierung muss alle vorhandenen Signaturen umschließen. Nur so lässt sich die Gesamtstruktur des Dokumentes und der dazugehörigen Signaturen und Informationen erhalten. Da die Neusignierung lediglich als Sicherungsmittel dient, kann die Neusignatur beliebig viele Daten umschließen, das heißt z. B. mehrere zu unterschiedlichen Zeiten signierte Dokumente.

Zeitstempel sind technisch gesehen in der Regel ebenfalls elektronische Signaturen, deren sicherheitstechnische Eignung im Laufe der Zeit verloren gehen kann. Bevor dies geschieht, müssen diese Zeitstempel daher ebenfalls konserviert werden, indem ein erneuter Zeitstempel eingeholt wird.

§17 SigV unterscheidet nicht danach, ob der Hash-Algorithmus, der Signaturschlüssel-Algorithmus oder beide ihre Eignung verlieren. Der qualifizierte Zeitstempel muss sich aber nur dann sowohl auf die signierten Daten als auch auf die Signatur beziehen, wenn der verwendete Hash-Algorithmus unsicher zu werden droht. Falls der Hash-Algorithmus noch geeignet ist, muss sich der zu bildende Zeitstempel nur auf die Signatur beziehen.

3.1.3 Sachbezogene rechtliche Regelungen an die Aufbewahrung von Akten der Verwaltung

Die allgemeine Dokumentationspflicht umfasst die Pflicht der Behörde, ordnungsgemäße Akten zu führen und alle wesentlichen Vorgänge, die für das Verwaltungsverfahren während seiner Durchführung und später für seine Nachvollziehbarkeit relevant sind, in Niederschriften oder Aktenvermerken festzuhalten, Schriftwechsel aufzubewahren und den gesamten Vorgang aktenkundig zu machen. Dies gilt auch für elektronisch erstellte oder erfasste Dokumente. Die ordnungsgemäße Aktenführung ist Voraussetzung für Kontrollen zur Rechtmäßigkeit des Verwaltungshandelns durch weisungsberechtigte Behörden, der Gewährung von Akteneinsicht der Verfahrensbeteiligten bzw. mittels der Akten die Unrechmäßigkeit beweisen zu können.

Besonders beweisrelevante Teile der Akte sind nach den Regelungen des VwVfG mit einer qualifizierten elektronischen Signatur zu versehen.

3.2 Funktionale Anforderungen an eine vertrauenswürdige elektronische Aufbewahrung

Vertrauenswürdige elektronische Langzeitspeichersysteme müssen folgende, sowohl rechtlich als auch funktional bestimmte Anforderungen wie Verfügbarkeit und Lesbarkeit, die Integrität und Authentizität sowie Datenschutz und Datensicherheit der gespeicherten elektronischen Informationen umsetzen.

3.2.1 Verfügbarkeit und Lesbarkeit

Langzeitspeichersysteme müssen die zur Aufbewahrung bestimmten Daten und Dokumente für die Dauer der gesetzlichen Aufbewahrungsfristen in Form und Inhalt authentisch und vollständig verkehrsfähig aufbewahren. Für die Sicherung der Verkehrsfähigkeit sind eindeutig interpretierbare Nutzdatenformate, deren Spezifikation standardisiert und öffentlich zugänglich ist, zu verwenden.

Physikalisch wie technologisch können Datenträger veralten und damit zu einer Nichtlesbarkeit der abgelegten Daten und Dokumente führen. Um dies zu verhindern, sind Datenträger vor Ablauf der vom Hersteller des Speichermediums zugesagten Haltbarkeitsfrist auf ihre Lesbarkeit zu überprüfen und gegebenenfalls auf neue Datenträger zu kopieren bzw. in neue aktuelle Datenformate zu übertragen. Verfügbarkeitsrisiken des Langzeitspeichersystems sind durch regelmäßige Datensicherungen zu minimieren.

3.2.2 Integrität und Authentizität

Die im Langzeitspeichersystem aufbewahrten Dokumente und Daten sind so zu erhalten, wie sie ursprünglich abgefasst worden sind, d. h. ohne nachträgliche Änderung und der Möglichkeit, auch nach langer Zeit den Aussteller des Dokumentes zweifelsfrei bestimmen zu können.

Eine wesentliche Aufgabe der Langzeitspeichersysteme ist es, die Integrität (Unveränderheit) und die Authentizität (eindeutige Zuordnung des Ausstellers) elektronisch aufbewahrter Daten und Dokumente nachzuweisen.

Dazu müssen elektronische Langzeitspeichersysteme in der Lage sein, qualifizierte elektronische Signaturen und Zeitstempel in der durch Rechtsvorschriften geforderten Qualität si-

cher und zuverlässig zu erzeugen, zu prüfen, zu erneuern und aufzubewahren. Die zur Signaturverifikation erforderlichen Verifikationsdaten sind gemeinsam mit den zu archivierenden Daten und Dokumenten für den maßgeblichen Aufbewahrungszeitraum verfügbar und in verkehrsfähiger Form abzulegen. Der Signaturzeitpunkt sollte grundsätzlich aus einem vertrauenswürdigen Zeitstempel entnommen werden.

Langzeitspeichersysteme sollten in der Lage sein, die Integrität nicht signierter Daten ab dem Zeitpunkt der Überführung in ein elektronisches Langzeitspeichersystem automatisch durch Eingangs-Hashwerte oder -signaturen und -zeitstempel zu sichern.

3.2.3 Datenschutz und Datensicherheit

Die Aufbewahrung elektronischer Informationen unterliegt allgemeinen bzw. bereichsspezifischen datenschutzrechtlichen Regelungen und Anforderungen. Es muss sichergestellt werden, dass Unbefugte unter keinen Umständen Zugang zu personenbezogenen oder anderweitigen dem Geheimnisschutz unterliegenden Daten erhalten.

3.3 Anwendungsorientierte funktionale Anforderungen

Anwendungsorientierte funktionale Anforderungen legen fest, über welche Funktionen ein Langzeitspeichersystem aus Sicht eines Benutzers verfügen sollte. Dabei werden folgende grundsätzliche Anwendungsfälle unterschieden:

- die Ablage signierter/unsignierter Daten,
- der Abruf gespeicherter Daten,
- der Abruf beweisgeeigneter Nachweise über die Authentizität und Integrität der aufbewahrten Daten und
- das Löschen von Daten.

Zugriffe auf das Langzeitspeichersystem sind in jedem Falle zu protokollieren und unberechtigte Zugriffe zuverlässig zu verhindern. Die an das Langzeitspeichersystem übergebenen Speicherobjekte sind auf Konformität mit den für das Langzeitspeichersystem durch den Betreiber eines Langzeitspeichersystems definierten und spezifizierten Datenformaten zu prüfen und gegebenenfalls die Ablage im Langzeitspeichersystem zu verweigern.

Signierte Daten sind vor Übergabe an das Langzeitspeichersystem umfassend zu prüfen und die Prüfergebnisse gemeinsam mit den signierten Daten abzulegen. Ein vertrauenswürdiges und rechtssicheres Langzeitspeichersystem muss im Stande sein, eine gesetzeskonforme Signaturerneuerung über sämtliche im Langzeitspeicher aufbewahrten, elektronisch signierten Daten und Dokumente durchzuführen. Der dauerhafte Nachweis der Integrität unsignierter Daten und Dokumente, zumindest ab dem Zeitpunkt des Übergangs in das Langzeitspeichersystem, soll durch einen elektronischen Eingangs-Hashwert, eine elektronische Eingangs-Signatur bzw. einen elektronischen Eingangs-Zeitstempel sichergestellt werden.

3.4 Technische Anforderungen

Eingesetzte Verfahren und technische Lösungen zur Langzeitspeicherung signierter elektronischer Daten dürfen die weitere Verwendbarkeit der elektronischen Dokumente nicht beeinträchtigen. Zur Sicherung einer dauerhaften Verfügbarkeit und Verkehrsfähigkeit der zu speichernden Daten und Dokumente sind ausschließlich Speicherformate einzusetzen, die eine plattform- und herstellerunabhängige Langzeitspeicherung ermöglichen.

3.4.1 Signaturerstellung

Das Erstellen einer Signatur erfolgt mittels einer Signatursoftware (z. B. Governikus Signer) in drei Schritten:

1. Berechnung des Hashwerts
   Für die Datei wird eine Funktion (Hashfunktion) angewendet, die einen eindeutigen Wert (Hashwert) erzeugt. Eine Hashfunktion ist ein kryptographischer Algorithmus, bei dem elektronische Nachrichten beliebiger Länge auf einen Hashwert fester Länge abgebildet werden. Ein Hashwert ist für jede Datei einmalig. Wird die Datei verändert, entsteht bei Anwendung der gleichen Hashfunktion ein anderer Wert.
2. Verschlüsselung des Hashwerts
   Für die Verschlüsselung des Hashwerts wird ein Schlüsselpaar, bestehend aus einem privaten (geheimen) und einem öffentlichen Schlüssel verwendet. Mit dem privaten Schlüssel wird der Hashwert verschlüsselt. Dazu wird von der Signatursoftware der Hashwert errechnet und dann an die Signaturkarte zur Verschlüsselung übergeben.

   Um den Missbrauch einer Signaturkarte zu verhindern, wird vor dem Verschlüsseln mit dem privaten Schlüssel eine persönliche Identifikationsnummer (PIN) abgefragt. Erst nach korrekter PIN-Eingabe wird die Verschlüsselung durchgeführt.
3. Hinzufügen des Zertifikats
   Nach Rückgabe des verschlüsselten Hashwerts an die Signatursoftware wird das Zertifikat von der Signaturkarte als Kopie dem verschlüsselten Hashwert hinzugefügt. Das Zertifikat enthält unter anderem den Namen des Signaturkarteninhabers, den öffentlichen Schlüssel und die Zertifizierungsstelle, die die Signaturkarte ausgestellt hat. Zudem wird der Verschlüsselungszeitpunkt hinzugefügt.

Der verschlüsselte Hashwert, das Zertifikat mit öffentlichem Schlüssel und der Verschlüsselungszeitpunkt bilden die elektronische Signatur.

3.4.2 Dokumentenformate

Für die dauerhafte Speicherung von Dokumenten sollten nur einige wenige Formate zur Anwendung kommen. Das Nebeneinander unterschiedlicher Formate in einem elektronischen Langzeitspeichersystem erhöht die Gefahr, dass einzelne Datentypen in Zukunft nicht mehr originalgetreu reproduziert werden können.

- TIF (Tagged Image File Format)
  Wird angewendet, wenn die Grafikinformation von entscheidender Bedeutung für die Aussagekraft eines Dokumentes ist und keine Notwendigkeit besteht, die Textinformationen des Dokumentes als intelligente Informationen (Volltextauszug) und als Bestandteil der Datei mitzuspeichern. Das TIF-Format wird vorwiegend für das Speichern von nur in Papierform vorliegenden Dokumenten eingesetzt, die durch Scannen in ein digitales Datenformat überführt werden und anschließend manuell indexiert werden.
- JPEG (Joined Photographic Experts Group)
  Standardformat für das Speichern und Austauschen von Bildern. Ermöglicht die Änderung des Komprimierungsgrades und Angabe der Dichte, so dass ein Kompromiss zwischen Dateigröße und Qualität in Abhängigkeit des Verwendungszwecks gefunden werden kann.

- PNG (Portable Network Graphics)
  Das Format unterstützt Transparenz, verlustfreie Kompression, inkrementelle Anzeige der Grafik (während des Ladens zunächst grobgerasterte Darstellung) und das Erkennen beschädigter Dateien.
- TXT (ASCII)
  Das Format stellt die größtmögliche Lesbarkeit sicher und ist daher für die Speicherung von Metadaten zu verwenden. Der Zeichensatz ist in der Norm ISO 8859-1 beschrieben.
- PDF (Portable Document Format)
  Das PDF-Format ermöglicht, neben der grafischen Information auch Textinformationen zu speichern, so dass beide Informationsebenen erhalten und nutzbar bleiben.

  Das PDF-Format ist besonders für die Speicherung von für nicht zur Veränderung vorgesehenen Dokumenten geeignet.
- PDF/A-Standard für die Langzeitspeicherung und das Archivieren elektronischer Dokumente
  PDF/A ist eine Normreihe der ISO zur Verwendung des PDF-Formats (Version 1.4) für die Langzeitarchivierung von elektronischen Dokumenten, veröffentlicht als ISO 19005-1:2005. PDF/A-Format bietet einen Mechanismus, der elektronische Dokumente auf solche Weise darstellt, dass das visuelle Erscheinungsbild über lange Zeit erhalten bleibt, unabhängig von Werkzeugen und Systemen zur Herstellung, Speicherung und Reproduktion. PDF/A-Konformität sichert sowohl eindeutige visuelle Reproduzierbarkeit wie auch Abbildbarkeit von Text nach Unicode und inhaltliche Strukturierung des Dokumentes. PDF/A-Dokumente dürfen weder direkt noch indirekt auf externe Quellen verweisen. Ein Beispiel dafür wäre ein externes Bild oder eine nicht im Dokument selbst eingebettete Schrift. PDF/A unterstützt die Einbettung von digitalen Signaturen.
- Multimedia-Formate
  Zunehmend werden auch Multimedia-Dateien Bestandteil elektronischer Akten, jedoch kann heute noch nicht abgesehen werden, welche der zahlreichen Formate sich langfristig am Markt behaupten werden.
- SGML/XML-basierte Dokumentenformate
  Ein Vorteil von XML ist die einfache Möglichkeit der strukturierten Recherche und Weiterverarbeitung durch Informationsextraktion.

  1. ODF (Open Document Format)
     Editierbares Format zum Dokumentenaustausch, standardisiert von ISO Nr.26300, implementiert in OpenOffice, Star Office, TYPO3, Google Docs
  2. OOXML (Office Open XML)
     Editierbares Format zum Dokumentenaustausch, standardisiert von Ecma International (ISO geplant), implementiert in MS Office ab Version 2007.

3.4.3 Speichermedien für Langzeitspeichersysteme

Die elektronische Speicherung erfordert Hard- und Softwarekomponenten, die aufeinander abgestimmt sein müssen und sicherstellen, dass die zum Lesen der Daten erforderliche Hardware noch lange verfügbar ist. Heute finden drei grundsätzlich verschiedene Typen von Speichermedien Verwendung: magnetische, optische und magneto-optische Speichermedien.

Magnetische Speicher:

Magnetische Speicher können beliebig oft überschrieben werden und zeichnen sich durch schnellen Zugriff und großer Speicherkapazität aus. Sie weisen jedoch eine begrenzte Lebensdauer auf. Typische Vertreter sind Magnetband und Festplattensysteme. Ein unbeabsichtigtes Löschen der Daten oder deren Manipulation kann bei magnetischen Speichern nicht ausgeschlossen werden.

Optische Speicher

Optische Speicher sind von Laser abgetastete digitale Speicher. Typische optische Speicher sind CD-ROM, WORM-Medien (write once, read many) und DVD-R. Diese Medien können nur einmal beschrieben werden und sichern somit die Unveränderbarkeit der auf dem Medium abgespeicherten Daten.

Magneto-optische Speicher MO/WORM

Bei der magneto-optischen Speicherung werden magnetische und optische Verfahren kombiniert. Im Gegensatz zu traditionellen magnetischen Speichern reicht zum Beschreiben magneto-optischer Medien das Anlegen eines Magnetfeldes allein nicht aus. Auf Grund des verwendeten Oberflächenmaterials ist eine Magnetisierung (Datenbeschreibung - Polarisierung der Oberflächenbeschichtung) erst dann möglich, wenn das Speichermedium, optisch mit Hilfe eines Laserstrahls punktuell und kurzzeitig erhitzt wird. Magneto-optische Speicher bieten gegenüber den optischen Speichern eine höhere physikalische Datensicherheit (Zuverlässigkeit).

4 Komponenten eines Langzeitspeichersystems

Nachfolgend werden die wichtigsten Komponenten eines elektronischen Langzeitspeichersystems dargestellt.

Medienverwaltung

Stellt Informationen zum Speicherort der angefragten Dokumente und Daten bereit. Zusätzlich können in dieser Datenbank beschreibende Informationen über den Inhalt der verwalteten Medien strukturiert abgelegt werden, wie Mediennummer, Medientyp, Speicherkapazität und allgemeine Inhaltsinformationen (z. B. Dokumente des Jahrgangs xx).

Indexdatenbank

Die Indexdatenbank enthält Metainformationen zu den abgelegten Dokumenten. Diese ermöglicht es den Nutzern eines Langzeitspeichersystems, gezielt auf die gespeicherten Dokumente und Daten zuzugreifen. Die festgelegte Metadatenstruktur bestimmt wesentlich die Recherchemöglichkeit innerhalb des Systems.

Volltextdatenbank

Die Volltextdatenbank beinhaltet komplette Volltextinformationen der gespeicherten Objekte. Dies umfasst in der Regel sowohl die Metainformationen, als auch die Primärinformationen

von Dokumenten. Als Ergebnis einer Suche in einer Volltextdatenbank liefert die Anwendung eine Liste derjenigen Objekte zurück, in denen die Zeichenkette gefunden wurde.

Benutzerverwaltung

Über die Benutzerverwaltung wird die Zuweisung von Nutzungsrechten auf einzelne Benutzer bzw. Benutzergruppen vorgenommen. Die Benutzerverwaltung umfasst damit neben der Speicherung von Benutzerinformationen und Passwörtern auch die Verwaltung von Zugriffsrechten auf die gespeicherten Objekte und die Definition frei konfigurierbarer Nutzerprofile, die beispielsweise nur die Ausübung ganz bestimmter Funktionen des Langzeitspeichersystems ermöglichen.

Clients

Ein Langzeitspeichersystem kann über unterschiedliche Zusatzmodule verfügen, deren Funktionalität an entsprechenden Arbeitsplätzen (Client-Arbeitsplätze) bereitgestellt wird (z. B. Scan-Client, Index-Client, Viewer).

5 Normen, Standards und Konzepte für die Schriftgutverwaltung

Bei den nachfolgend aufgeführten Normen, Standards und Konzepten handelt es sich nicht um Rechtsnormen. Sie sind daher grundsätzlich nicht bindend, sondern stellen eine Orientierungshilfe bei der Bestimmung von Anforderungen an ein Langzeitspeichersystem dar.

DIN ISO 15489

ISO 15489 ist die internationale Norm für die Schriftgutverwaltung. Ziel der Norm ist

- die angemessene Berücksichtigung und der notwendige Schutz aller Unterlagen,
- das effektive und effiziente Wiederauffinden und Nachweisen von Informationen in Dokumenten,
- die klare Benennung von Zuständigkeiten und Verantwortlichkeiten in der Schriftgutverwaltung.

Die Norm berücksichtigt alle Medien und Formate der Schriftgutverwaltung, d. h. auch die elektronischen Medien. Die Verwaltung und Aufbewahrung von Unterlagen in Archiven wird nicht betrachtet.

www.iso.org

MoReq (Model Requirements for the management of electronic documents and records)

MoReq ist eine technische Spezifikation für die Entwicklung, Beschaffung und Implementierung von Dokumentenmanagementsystemen (DMS). Sie wurde von der EU-Kommission in Auftrag gegeben und erstmals 2001 veröffentlicht. Die ergänzte und erweiterte Version MoReq2 erschien im Februar 2008 und gilt europaweit als de-facto-Standard, in dem funktionale Anforderungen zur Verwaltung elektronischer Unterlagen in Dokumentenmanagementsystemen genannt werden. Organisatorische Anforderungen oder Regelungen zum Geschäftsgang werden nicht formuliert.

www.moreq2.eu

ERS (Evidence Record Syntax) Standard

ERS ist ein von der IETF (Internet Engineering Task Force) entwickelter und international gültiger Standard, welcher im Detail definiert, wie Signaturerneuerungen für große Dokumentenmengen automatisch, unbegrenzt und sicher durchgeführt werden können.

http://tools.ietf.org/html/rfc4998

DOMEA (Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang)

Das DOMEA-Konzept „Papierarmes Büro“ wurde 1999 erstmals veröffentlicht und gilt seither als Quasi-Standard für die elektronische Vorgangsbearbeitung in Deutschland. Die aktuell gültige Version DOMEA 2.1 vom November 2005 umfasst das Organisationskonzept, elf Erweiterungsmodule, den Anforderungskatalog sowie das Zertifizierungsverfahren. Als thematischen Schwerpunkt behandelt das Organisationskonzept den Geschäftsgang unter ablauforganisatorischen Aspekten. Ein Geschäftsgang wird wie folgt beschrieben:

Eingangsbehandlung – Bearbeitung – Postausgang – Archivierung. Zu jedem der genannten Bereiche befasst sich das Organisationskonzept grundsätzlich mit der Darstellung des Ist-Zustandes, der Beschreibung der Probleme sowie der Darstellung organisatorischer Lösungsansätze und technischer Umsetzungsmöglichkeiten.

www.kbst.bund.de

ArchiSig

Das Konzept ArchiSig beschreibt ein Verfahren für die sichere und beweiskrafterhaltende, langfristige Speicherung/Archivierung digital signierter Dokumente. Unter Berücksichtigung existierender Standards werden technische Komponenten und Schnittstellen sowie organisatorische Konzepte von Public Key-Infrastrukturen unter Einbindung von Dokumentenmanagement- und Archivierungssystemen spezifiziert.

www.archisig.de

TransiDoc

TransiDoc (Transformation signierter Dokumente) ist ein Konzept, das Anforderungen und Regeln (Normen) für die rechtssichere Transformation elektronisch signierter Dokumente spezifiziert.

www.transidoc.de

TR-VELS (Technische Richtlinie zur vertrauenswürdigen elektronischen Langzeitspeicherung BSI TR – 03125)

Beschreibt auf der Grundlage bestehender rechtlicher Normen und technischer Standards sowie nationaler und internationaler Erfahrungen Anforderungen und Kriterien für die langfristige, rechts- und revisionssichere Aufbewahrung elektronischer Dokumente.

https://www.bsi.bund.de/cln_183/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html

6 Produktlösungen zur Neusignierung von elektronischen Dokumenten

Die Reihenfolge der Produktnennungen stellt keine Wertung dar, auch erhebt die Auflistung keinen Anspruch auf Vollständigkeit.

ArchiSoft

Das vom Fraunhofer-Institut SIT entwickelte Softwarepaket ArchiSoft aktualisiert Signaturen bei Bedarf, bevor sie veralten. Die Software kann von den meisten DMS-Servern durch Einbinden eines Plug-In genutzt werden. Unternehmen, die keinen eigenen ArchiSoft-Server betreiben möchten, können bei SIT-Partnern ArchiSoft als Service nutzen.

http://www.sit.fraunhofer.de/forschungsbereich/tad/archisoft.jsp

OpenLimit OverSign

Mit OpenLimit OverSign erneuern Sie elektronische Signaturen auf Dokumenten, die langfristig gespeichert und den gesamten Zeitraum die gesetzliche Beweiskraft erhalten müssen. Standardisierte Datenformate und Protokolle gewährleisten das reibungslose Zusammenspiel von OpenLimit OverSign mit unterschiedlichsten Applikationen.

http://www.openlimit.com/de/produkte/oversign.html

Hash-Safe

Hash-Safe realisiert einen Signaturlangzeitspeicher/-Archiv, dazu werden Hashbäume erzeugt, welche die Datenbestände eines Tages, Monats oder Jahres repräsentieren. Die Signaturdaten werden parallel zu den Dokumenten in einem DMS- oder Archivsystem gesondert gespeichert.

http://mentana-claimsoft.de/hash-safe-archisig.html

digiSeal archive

Die Softwarelösung digiSeal archive signiert auf Basis des ArchiSign-Konzepts vorhandene signierte Daten rechtzeitig, sicher und effizient nach. Dabei setzt sie international gültige Standards ein und verwendet gesetzeskonforme amtliche Zeitstempel.

http://www.secrypt.de/produkte/digiseal-archive/

SecDocs

Mit SecDocs bieten Fujitsu und OpenLimit eine Lösung für die vertrauenswürdige Langzeitspeicherung/-Archivierung auf Basis der Technischen Richtlinie 03125 (TR-VELS). Die Lösung wurde durch das Bundesamt für Sicherheit in der Informationstechnik zertifiziert.

http://de.ts.fujitsu.com/

Elektronische Langzeitspeicherung mit Governikus und IBM

Auf Basis von Governikus haben die bos-bremen gemeinsam mit IBM eine Lösung für die Langzeitspeicherung von Dokumenten und Akten entwickelt. Die Beweiswerterhaltung der Dokumente wird dabei durch den Einsatz von qualifizierten Signaturen und Zeitstempeln sowie die Trennung zwischen Dokumenten- und Beweis-Archiv sichergestellt.

http://www.bos-bremen.de/fastmedia/477/Governikus_Langzeitspeicherung.pdf

7 Glossar

Archivierung

Archivierung ist die dauerhafte und unveränderbare Aufbewahrung (Speicherung) von elektronischen Dokumenten und Daten. Archivierung im juristischen Kontext betrifft allein Unterlagen der öffentlichen Verwaltung und bezieht sich darauf, dass Schriftgut einer zuständigen Behörde ausgesondert und „ewig“ verwahrt werden soll.

Attributzertifikat

Ein Attribut steht für eine besondere Eigenschaft, Stellung oder Beschränkung des Zertifikatsinhabers (berufsbezogene Angaben, Beschränkungen, Vertretungsmacht für eine natürliche oder juristische Person).

Authentizität

Elektronische Daten sind authentisch, wenn sie mit den Ursprungsdaten übereinstimmen und ihnen zweifelsfrei die Identität eines Ausstellers (Verfassers, Erstellers oder Absenders) zugeordnet werden kann.

Beweisdaten, technisch

Technische Beweisdaten dienen dem Nachweis der Unversehrtheit der Integrität und Authentizität der gespeicherten Daten. In Übereinstimmung mit den Spezifikationen des ERS-Standards der IETF enthält ein technischer Beweisdatensatz Zeitstempel ausreichender Qualität über die gespeicherten (signierten) Daten, die die Unversehrtheit der Daten nachweisen, und zusätzlich Informationen, welche die Richtigkeit und die Gültigkeit elektronischer Signaturen zum Signaturzeitpunkt sowie die rechtzeitige Signaturerneuerung entsprechend der rechtlichen Anforderungen belegen.

Beweisrelevante Daten

Beweisrelevante Daten sind Signaturen bzw. Zeitstempel zu genau einem Datenobjekt bzw. Dokument und enthalten auch die für die Prüfung der Signatur bzw. Zeitstempelsignatur notwendigen Prüfdaten.

Daten

Oberbegriff für alle Informationen, die von elektronischen Medien gelesen, elektronisch verarbeitet oder auf elektronische Medien gespeichert werden.

Dokument

Alle Arten von Informationen, die zur Wahrnehmung durch den Menschen bestimmt sind und als Einheit zwischen Systemen oder Benutzern ausgetauscht werden können. Bei elektronischen Dokumenten sind die Informationen maschinell lesbar und verarbeitbar und werden ganz allgemein als Daten bezeichnet.

Dokumenten-Management-System (DMS)

Oberbegriff für informationstechnische Systeme zur Verwaltung von Dokumenten von der Erfassung bis zur Archivierung.

Hashfunktion

Eine Hashfunktion ist ein kryptographischer Algorithmus, bei dem (elektronische) Nachrichten beliebiger Länge auf einen Hashwert fester Länge abgebildet werden.

Hashwert

Ein Hashwert ist eine eindeutige Prüfsumme elektronischer Daten. Der Hashwert wird durch Anwendung der Hashfunktion auf elektronische Daten gebildet.

Integrität

Elektronische Daten sind integer, wenn sie vollständig sind und nachweislich keine Veränderung oder Manipulation an den Daten festgestellt werden kann.

Elektronische Langzeitspeicherung

Sicherung des Direktzugriffes auf elektronische Dokumente der öffentlichen Verwaltung für den Zeitraum der gesetzlich festgelegten Aufbewahrungsfrist.

Metadaten

Informationen, die andere Informationen (z. B. ein Dokument) beschreiben. Es kann sich z. B. handeln um Eingangsdatum, Einsender, Ersteller, Aktenzeichen, Betreff, Ausgangsdatum, Dokumententyp. Welche Informationen als Metadaten ein Dokument beschreiben sollen, muss für ein DMS-System vereinbart werden.

OCSP (RFC 2560)

Das Online Certificate Status Protocol ist ein Protokoll für die Online-Statusabfrage eines elektronischen Zertifikats bei einem Zertifizierungsdiensteanbieter.

Verkehrsfähigkeit

Verkehrsfähigkeit bezeichnet die Möglichkeit, dass elektronische Daten und Dokumente technisch unverändert auf den zum Zeitpunkt ihrer in Verkehrsbringung üblichen DV-Systeme lesbar angezeigt bzw. übertragen oder gespeichert werden können.

Vertraulichkeit

Vertraulichkeit bezeichnet den Schutz vor unbefugter Kenntnisnahme zur Sicherung personenbezogener Daten und betriebs- und berufsbezogener Geheimnisse.

Zeitstempel, elektronischer

Ein Zeitstempel ist eine von einem vertrauenswürdigen Dritten zuverlässig bescheinigte elektronische Angabe von Zeit und Datum. Ein Zeitstempel dient dazu, verlässlich und nachweislich zu belegen, dass digitale Daten eines bestimmten Inhalts zu einem bestimmten Zeitpunk bei einem Aussteller des Zeitstempels vorgelegen haben.

Zertifikat

Nach § 2 Nr. 6 SigG sind Zertifikate elektronische Bescheinigungen, mit denen Signaturschlüssel einer Person zugeordnet werden und die Identität einer Person bescheinigt wird.

Qualifizierte Zertifikate werden nur auf natürliche Personen ausgestellt. Das Zertifikat enthält neben dem öffentlichen Signaturschlüssel insbesondere Angaben zur Person, die von der ausstellenden Instanz zum Zeitpunkt der Zertifikatsausstellung geprüft wurden, sowie zum Gültigkeitszeitraum.