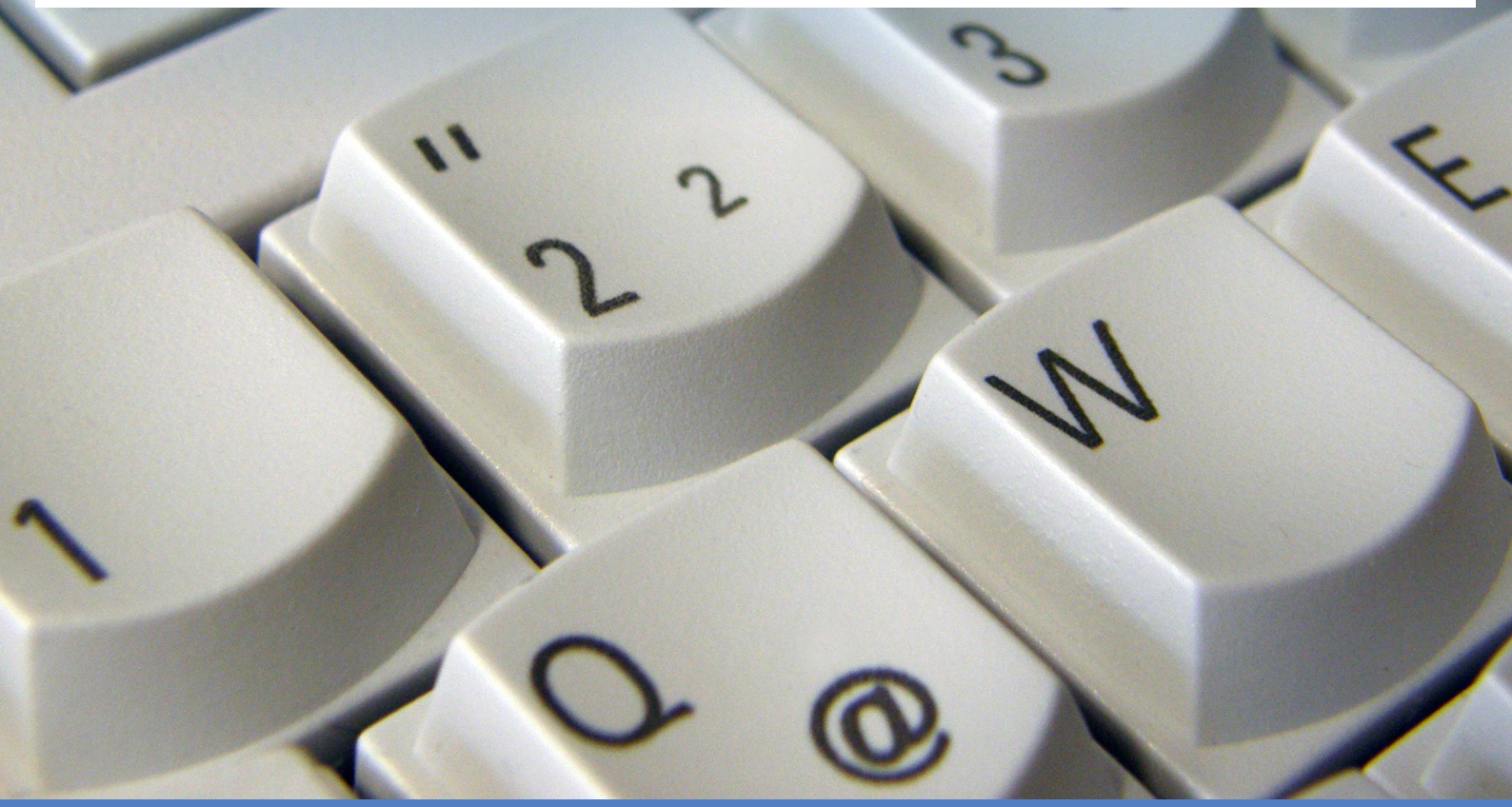
Bundesministerium
des Innern

vernetzt und transparent
verwaltung-innovativ.de

Organisationskonzept elektronische Verwaltungsarbeit

Baustein E-Poststelle



Baustein
E-Poststelle

Inhaltsverzeichnis

1 Einleitung

1.1 Zweck und Funktion des Bausteins

Der Baustein E-Poststelle dient als Orientierungshilfe für Behörden bei der Konzeption und Einführung der elektronischen Posteingangs- und -ausgangsbearbeitung.

Für ein solches Vorhaben sind die rechtlichen Rahmenbedingungen und die fachlichen Anforderungen an den Ein- und Ausgang von elektronischen Dokumenten festzustellen. Auf dieser Basis sind organisatorische als auch technische Überlegungen anzustellen. Aus technischer Sicht sind Fragen der technischen Infrastruktur, der benötigten Funktionalitäten und auch des technischen Betriebs zu klären. Aus organisatorischer Sicht ist zu klären, wie die Prozesse der elektronischen Posteingangs- und -ausgangsbearbeitung gestaltet werden sollen und wer in diesen Prozessen welche Aufgaben übernimmt.

Der Fokus dieses Bausteins liegt auf der Betrachtung der organisatorischen Aspekte[1]. Im Gegensatz zur Papierpost ist es dabei meist nicht zwingend erforderlich, eine spezielle Organisationseinheit „Poststelle“ einzurichten. Vielmehr gilt es, den Ein- und Ausgang von elektronischen Dokumenten organisatorisch und soweit sinnvoll auch technisch zu regeln. Da der Begriff „virtuelle Poststelle“ bereits mit einer technischen Lösung[2] verknüpft ist, die nur als *ein* Beispiel für die Umsetzung einer solchen Poststelle anzusehen ist, wird an dieser Stelle der Begriff „elektronische Poststelle“ verwendet.

Angesichts der Komplexität und Dynamik des Themas enthält der vorliegende Baustein keine umfassende Darstellung aller möglichen Kommunikationskanäle, Systeme und Organisationsformen. Vielmehr soll ein Überblick zu den Chancen und Herausforderungen bei der Organisation der elektronischen Kommunikation gegeben werden.

Die konkrete Umsetzung einer elektronischen Poststelle ist durch die jeweilige Behörde – unter Beachtung der behördenspezifischen Besonderheiten – individuell zu planen. Dabei sind die Rahmenbedingungen der jeweiligen Kommunikationspartner (wie z. B. Bürger, Unternehmen oder andere Behörden) zu beachten. Wenn möglich, ist eine Abstimmung mit diesen Kommunikationspartnern vorzusehen.

1 Für technische Fragen wird an verschiedenen Stellen des Bausteins auf die bereits vorhandenen Dokumentationen und Leitfäden verwiesen.

2 Wie z. B. die Virtuelle Poststelle des Bundes (https://www.bsi.bund.de/DE/Themen/weitereThemen/VirtuellePoststelle/virtuellepoststelle_node.html - Abruf 15.08.2013)

1.2 Einordnung in das Organisationskonzept elektronische Verwaltungsarbeit

Der Baustein E-Poststelle des Organisationskonzeptes elektronische Verwaltungsarbeit beschreibt die rechtlichen, fachlichen, funktionalen und organisatorischen Anforderungen an die elektronische Posteingangs- und -ausgangsbearbeitung. Im Anhang des Dokuments wird auf grundsätzliche Aspekte des Einsatzes elektronischer Signaturen sowie von De-Mail eingegangen.

Der Baustein E-Poststelle ergänzt die Aussagen in anderen Bausteinen des Organisationskonzeptes elektronische Verwaltungsarbeit um den Aspekt der sicheren und nachvollziehbaren Übertragung elektronischer Dokumente. Spezifische Fragestellungen der elektronischen Verwaltungsarbeit, z. B.

- zur E-Akte,
- zur E-Vorgangsbearbeitung,
- zur E-Zusammenarbeit,
- zum Scanprozess und
- zur E-Langzeitspeicherung

sind in separaten Bausteinen dargestellt. In den einzelnen Kapiteln des Bausteins E-Poststelle wird an den notwendigen Stellen auf die jeweils relevanten Bausteine verwiesen.

2 Grundlegende Anforderungen

2.1 Definitionen und Begriffe

Elektronische Kommunikation

Unter dem Begriff „Elektronische Kommunikation“ werden in diesem Baustein alle Formen der elektronischen Übertragung von Nachrichten verstanden (z. B. E-Mail). Dabei ist es unerheblich, auf welchem Weg (Kommunikationskanal) und in welcher Form die Daten übertragen werden.

Elektronische Poststelle (E-Poststelle)

Eine elektronische Poststelle im Sinne dieses Bausteins umfasst die Gesamtheit der Prozesse und Strukturen, die zur Bearbeitung der elektronischen Postein- und -ausgänge nötig sind[3]. Damit ist die E-Poststelle nicht zwangsläufig eine konkrete Organisationseinheit. Der Begriff beschreibt vielmehr eine virtuelle Organisation, in der verschiedene Beteiligte mit Hilfe von Informationstechnologie elektronische Ein- und Ausgänge bearbeiten (vgl. Kapitel 3).

E-Poststellen-Infrastruktur

Die technische Infrastruktur einer E-Poststelle umfasst die gesamte IT-Infrastruktur zur Bearbeitung von elektronischen Postein- und -ausgängen. Dabei handelt es sich meist nicht um ein einzelnes IT-System. Vielmehr setzt sie sich aus mehreren IT-Systemen wie z. B. E-Mail-Server, E-Fax-System, Web-Portal zusammen. Darüber hinaus kann die Poststellen-Infrastruktur auch ein System zur Bündelung der verschiedenen Kommunikationskanäle beinhalten.

Elektronische Signatur

Elektronische Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten (z. B. Dokumenten) beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen (§ 2(1) SigG). Die Signaturerstellerin oder der Signaturersteller kann mit Hilfe dieser Daten identifiziert und die Integrität der Dokumente/Daten kann geprüft werden. Die Systematik, die Begrifflichkeiten und die Voraussetzungen zur Nutzung elektronischer Signaturen werden im Signaturgesetz und in der Signaturverordnung geregelt. Man unterscheidet zwischen

- [einfachen] elektronischen Signaturen,
- fortgeschrittenen elektronischen Signaturen und
- qualifizierten elektronischen Signaturen.

Weitere Informationen zu elektronischen Signaturen finden sich in Anlage 2 „Elektronische Signatur“.

3 Unter Prozessen und Strukturen werden die Ablauforganisation, die Aufbauorganisation und auch die IT-Strukturen verstanden.

2.2 Rechtliche Anforderungen an die E-Poststelle

Wesentliches Ziel der E-Poststelle ist die Bereitstellung geeigneter elektronischer Kanäle für die verschiedenen Kommunikationsbedarfe. Für die vertrauenswürdige Kommunikation sollen daher Kanäle zur Verfügung gestellt werden, mit denen Bürgerinnen und Bürger, Wirtschaft sowie Verwaltungsorganisationen auf elektronischem Wege sicher und nachvollziehbar mit der Verwaltung kommunizieren und z. B. Dokumente austauschen können.

Vor diesem Hintergrund sind bei der Einrichtung und dem Betrieb elektronischer Poststellen eine Reihe rechtlicher Anforderungen zu beachten. Im Folgenden werden die wesentlichen zu beachtenden Rechtsnormen kurz aufgeführt.

2.2.1 Bürgerliches Gesetzbuch (BGB)

Bei der Planung und Umsetzung einer E-Poststelle sind aus dem BGB insbesondere Vorschriften zur Form von Willenserklärungen zu berücksichtigen, d. h. es ist zu beachten, in welcher Form Informationen (z. B. Dokumente) im privatrechtlichen Geschäftsverkehr übergeben bzw. übertragen werden müssen. Dabei gilt grundsätzlich, dass keine bestimmte Form vorgegeben ist. Allerdings werden im BGB Ausnahmen mit Formvorgaben genannt. Dies sind insbesondere die Schriftform (§ 126 Abs. 1 BGB), die elektronische Form (§ 126a BGB) und die Textform (§ 126b BGB)[4].

Aus diesen Formvorschriften lassen sich sowohl fachliche als auch technische Anforderungen an eine E-Poststelle ableiten. Beispielsweise sollte aus funktionaler Sicht die technische In-frastruktur der E-Poststelle in der Lage sein, elektronische Nachrichten bzw. Dokumente mit Schriftformerfordernis zu verarbeiten.

2.2.2 Zivilprozessordnung (ZPO)

Bei Gerichten können Schriftsätze und deren Anlagen, für welche die Schriftform vorgesehen ist, als elektronisches Dokument eingereicht werden, wenn die verantwortende Person das Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versieht und es für die Bearbeitung durch das Gericht geeignet ist (vgl. § 130a ZPO). Darüber hinaus ist geregelt, dass ein elektronisches Dokument als eingereicht gilt, sobald die für den Empfang bestimmte Einrichtung des Gerichts, d. h. die E-Poststelle, es aufgezeichnet hat.

Mit dem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten werden die Regelungen der ZPO schrittweise[5] angepasst. Dabei werden die Vorgaben zur Übertragung elektronischer Dokumente konkretisiert und es wird die Nutzung von Übertragungswegen (wie z. B. De-Mail) und die Bestätigung von Eingängen geregelt.

2.2.3 Verwaltungsverfahrensgesetz (VwVfG)

Das Verwaltungsverfahrensgesetz (VwVfG) regelt die Durchführung von Verwaltungsverfahren. Im Zusammenhang mit dem Thema E-Poststelle ist insbesondere der § 3a VwVfG (Elektronische Kommunikation) zu beachten.

Danach ist die Übermittlung elektronischer Dokumente an eine Behörde zulässig, wenn diese hierfür einen Zugang eröffnet. Die Zugangseröffnung, die die wesentliche Voraussetzung für die Kommunikation mit der Verwaltung ist, regelt sich nach den § 3a Abs. 1 VwVfG, § 87a Abs. 1 AO oder § 36a Abs. 1 SGB I. Danach kann nur mittels wirksamer Zugangseröffnung die Übermittlung von elektronischen Daten und Dokumenten (z. B. mittels De-Mail) stattfinden. Ist bei einem elektronischen Dokument die Schriftform vorgeschrieben, ist nach § 3a Abs. 2 VwVfG zudem eine qualifizierte elektronische Signatur nach dem Signaturgesetz anzubringen. Die Schriftform kann ersetzt werden, wenn

- eine Erklärung unmittelbar in einem elektronischen Formular erfolgt, welches von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird[6],
- die Erklärung in Form einer De-Mail-Nachricht mit der Versandoption „absenderbestätigt“ übertragen wird[7] oder
- sonstige sichere Verfahren, die durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates festgelegt werden, genutzt werden.

4 Vgl. Bundesministerium des Innern (BMI), Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Akte, Kapitel 2.3, Berlin, Mai 2012

5 Das Gesetz zur Förderung des elektronischen Rechtsverkehrs tritt schrittweise in Kraft.

6 Hierbei muss ein sicherer Identitätsnachweis nach § 18 PauswG (eID-Funktion) erfolgen.

7 Dabei handelt es sich um De-Mail-Nachrichten, bei denen der Versender zum Zeitpunkt des Versands dieser De-Mail mit hohem Authentisierungsniveau angemeldet war (§ 5 Abs. 5). Vgl. auch BSI, BSI TR 01201 Teil 3.1

Kann eine Behörde ein übermitteltes elektronisches Dokument nicht bearbeiten, muss die Behörde den Absender informieren. In solchen Fällen muss dem Absender mitgeteilt werden, unter welchen technischen Rahmenbedingungen (z. B. Formate) eine Bearbeitung möglich ist. Falls ein Empfänger ein von der Behörde empfangenes elektronisches Dokument nicht bearbeiten kann, muss die Behörde es ihm erneut in einem geeigneten elektronischen Format[8] oder als Papierschriftstück zusenden.

2.2.4 Verwaltungszustellungsgesetz (VwZG)

Das Verwaltungszustellungsgesetz (VwZG) regelt das Zustellungsverfahren von Bundesbehörden, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts und der Landesfinanzbehörden.

Zugestellt wird, soweit dies durch Rechtsvorschrift oder behördliche Anordnung vorgegeben ist. Ähnliche Normen gibt es auch für die Bundesländer. Dabei bedeutet „Zustellung“ nach § 2 VwZG, dass dem Empfänger ein schriftliches oder elektronisches Dokument nachvollziehbar übermittelt, d. h. bekanntgegeben, wird. Die Zustellung kann dabei u. a. in den folgenden Formen erfolgen:

- Zustellung durch die Post mit Zustellungsurkunde (§ 3 VwZG),
- Zustellung durch die Post mittels Einschreiben (§ 4 VwZG),
- Zustellung durch die Behörde gegen Empfangsbekenntnis; elektronische Zustellung (§ 5 VwZG) und
- elektronische Zustellung gegen Abholbestätigung über De-Mail-Dienste (§ 5a VwZG).

Für die E-Poststelle bedeutet dies u. a., dass mit der Nutzung von De-Mail eine elektronische Zustellung gegen Abholbestätigung möglich ist, welche eine Zustellung gegen Empfangsbekenntnis ersetzen kann.

2.2.5 E-Government-Gesetz

Das Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (E-Government-Gesetz - EGovG) dient dem Ziel, die elektronische Kommunikation mit der Verwaltung zu erleichtern und Bund, Ländern und Kommunen zu ermöglichen, einfachere, nutzerfreundlichere und effizientere elektronische Verwaltungsdienste anzubieten. Das Gesetz ist in wesentlichen Teilen am 1. August 2013 in Kraft getreten. Mit diesem Gesetz wurden die rechtlichen Rahmenbedingungen der Verwaltungsarbeit umfassend geändert. Behörden sollen auf der Grundlage des EGovG umfassender elektronisch arbeiten und grundsätzlich elektronische Akten führen. Weiterhin müssen beispielsweise eine elektronische Bezahlmöglichkeit und die elektronische Akteneinsicht angeboten werden.

Aus Sicht der elektronischen Posteingangs- und -ausgangsbehandlung sind insbesondere die Verpflichtung der Bundesverwaltung zur Einrichtung eines elektronischen Zugangs und die Änderung der Schriftformregelungen zu berücksichtigen[9]. So kann die Schriftform neben der qualifizierten elektronischen Signatur nunmehr auch durch zwei weitere sichere Technologien ersetzt werden:

1. De-Mail mit der Versandoption „absenderbestätigt“, welche eine „sichere Anmeldung“ voraussetzt und
2. Web-Anwendungen der Verwaltung in Verbindung mit sicherer elektronischer Identifizierung durch die eID-Funktion des neuen Personalausweises.

Außerdem erlaubt eine Rechtsverordnungsermächtigung der Bundesregierung mit Zustimmung des Bundesrates die rasche Anpassung an die deutschland- wie europaweite technologische Weiterentwicklung. Mit der Rechtsverordnung können weitere ausreichend sichere Verfahren als Schriftformersatz festgelegt werden.

2.2.6 Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten

Das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten wurde Anfang Juli 2013 durch den Bundesrat gebilligt. Mit diesem Gesetz wird der elektronische Zugang zur Justiz durch entsprechende bundeseinheitliche Regelungen in der ZPO und in anderen Verfahrensordnungen erweitert.

Übergeordnete Zielstellung des Gesetzes ist die Schaffung von rechtlichen Rahmenbedingungen zur Anerkennung von elektronischen Dokumenten seitens der Gerichte. Es ermöglicht die Kommunikation mit der Justiz ohne qualifizierte elektronische Signatur, wenn die Übertragung über De-Mail, über ein besonderes elektronisches Rechtsanwalts- oder Behördenpostfach oder über einen anderen sicheren Kommunikationsweg erfolgt[10].

8 Vgl. hierzu: Die Beauftragte der Bundesregierung für Informationstechnik (BfIT), SAGA-Modul Technische Spezifikationen, Version de.bund 5.0.0, 3. November 2011, Kapitel 7

9 Vgl. Artikel 1 § 2 EGovG und Artikel 3 Abs. 1 EGovG.

10 Das Gesetz tritt gestaffelt in Kraft. In einem ersten Schritt sind ab 1. Juli 2014 Möglichkeiten zur Nutzung elektronischer Formulare und zur elektronischen Zustellung zu schaffen.

Für Behörden bedeutet dies, dass bei der Abwicklung von elektronischer Kommunikation in Verwaltungsangelegenheiten (insbesondere mit den Bürgerinnen und Bürgern) den im Kapitel 2.3 beschriebenen fachlichen Anforderungen besondere Aufmerksamkeit zu schenken ist. Aus technischer Sicht ergibt sich aus den Gesetzesänderungen und der damit einhergehenden Ausweitung der elektronischen Kommunikation in rechtlichen Angelegenheiten die Anforderung der Nutzung sicherer Systeme wie z. B. De-Mail[11].

2.2.7 De-Mail-Gesetz

Das De-Mail-Gesetz regelt die Bereitstellung und Nutzung von De-Mail-Diensten. Dies sind Dienste auf einer elektronischen Kommunikationsplattform, die einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen sollen. Diesbezüglich muss ein De-Mail-Dienst eine sichere Anmeldung, die Nutzung eines Postfach- und Versanddienstes für sichere elektronische Post sowie die Nutzung eines Verzeichnisdienstes aufweisen und kann zusätzlich auch Identitätsbestätigungs- und Dokumentenablagedienste ermöglichen. Der De-Mail-Dienst wird von nach dem De-Mail-Gesetz akkreditierten Diensteanbietern betrieben. Elektronische Kommunikationsstrukturen und sonstige Anwendungen, die der sicheren Übermittlung von Nachrichten und Daten dienen, bleiben unberührt.

Durch das E-Government-Gesetz wurde die Bedeutung von De-Mail erheblich gestärkt, da die Bundesbehörden zur Einrichtung eines De-Mail-Kontos verpflichtet sind (Artikel 1 § 2 EGovG). Bislang schriftlich zu erfolgende Erklärungen in der Verwaltungskommunikation können durch eine Übermittlung der Erklärung über De-Mail ersetzt werden (Artikel 3 Absatz 1 EGovG), sofern für den Zuständigkeitsbereich der Behörde nicht etwas anderes geregelt ist.

2.2.8 Signaturgesetz und Signaturverordnung

Das Signaturgesetz (SigG) regelt die Systematik, die Begrifflichkeiten und die Voraussetzungen zur Nutzung elektronischer Signaturen. Vor dem Hintergrund der Bedeutung von insbesondere qualifizierten elektronischen Signaturen bei Austausch elektronischer Dokumente sollte die E-Poststellen-Infrastruktur über Funktionen zur Prüfung und Anbringung (qualifizierter) elektronischer Signaturen verfügen[12]. Die qualifizierte elektronische Signatur entspricht der eigenhändigen Unterschrift auf einem Papierdokument. Daher erfüllt ein mit einer qualifizierten elektronischen Signatur versehenes Dokument die Schriftformerfordernis.

Die Signaturverordnung (SigV) ergänzt das Signaturgesetz speziell in den Anforderungen für die Zertifizierungsdiensteanbieter[13] und den Anforderungen für die Produkte, die im Zusammenhang mit der elektronischen Signatur verwendet werden dürfen. Diese Vorgaben sind bei der Planung und Einrichtung elektronischer Poststellen zu beachten[14].

2.2.9 Verwaltungsvorschriften

Neben den Gesetzen und Verordnungen sind für die öffentliche Verwaltung auch die entsprechenden Verwaltungsvorschriften zu beachten. In der Bundesverwaltung sind dies beispielsweise die Gemeinsame Geschäftsordnung der Bundesministerien und die Registraturrichtlinie.

2.2.9.1 Gemeinsame Geschäftsordnung der Bundesministerien (GGO)

In Umsetzung der Organisationsgrundsätze für die Bundesministerien enthält die Gemeinsame Geschäftsordnung der Bundesministerien (GGO) Maßgaben zu den elektronischen Informations- und Kommunikationssystemen. So sollen Bundesministerien gemäß § 5 Abs. 1 GGO die Voraussetzungen schaffen, um Informationen in elektronischer Form bereitzustellen, ressortübergreifend auszutauschen und zu nutzen. Weiterhin wird zwischen den Bundesministerien eine sichere ressortübergreifende Kommunikationsstruktur betrieben, um eine geschützte elektronische Kommunikation zu gewährleisten (§ 5 Abs. 2 GGO). Nach § 16 Abs. 3 GGO erfolgt der elektronische Schriftverkehr zwischen den Bundesministerien über die nach § 5 Abs. 2 GGO betriebene Kommunikationsstruktur.

Weiterhin ist für die E-Poststelle die Anlage 1 zu § 13 Abs. 2 GGO – die Behandlung von Eingängen – zu beachten. Darin ist festgelegt, dass elektronische Eingänge in der Regel elektronisch weiterzuleiten sind.

2.2.9.2 Registraturrichtlinie

Die Registraturrichtlinie (RegR) ist eine Verwaltungsvorschrift, die die GGO ergänzt und das Bearbeiten von Geschäftsvorfällen und Verwalten von Schriftgut in

11 Vgl. Anlage 1: Übersicht De-Mail

12 Für weitergehende Informationen zu Signaturen siehe Anlage 2: Elektronische Signatur

13 Zertifizierungsdiensteanbieter sind die in Deutschland tätigen juristischen Personen, die der Bundesnetzagentur gem. § 4 Abs. 3 SigG i.V.m. §§ 1, 2 der SigV das Ausstellen qualifizierter Zertifikate oder qualifizierter Zeitstempel angezeigt haben (vgl. Anlage 2).

14 Für weitergehende Informationen zu Signaturen siehe Anlage 2: Elektronische Signatur

Bundesministerien regelt. Zur sachgerechten und wirtschaftlichen Bearbeitung und Verwaltung von Schriftgut wird neben der papierbezogenen Bearbeitung die IT-gestützte Vorgangsbearbeitung und Verwaltung von elektronischen Dokumenten und Akten berücksichtigt. Soweit nichts anderes bestimmt ist, gelten daher die Regelungen auch für die elektronische Bearbeitung und Verwaltung von Schriftgut (§ 1 RegR).

2.3 Fachliche Anforderungen an eine E-Poststelle

In der Papierwelt ist es Aufgabe einer Poststelle, Eingänge in Bezug auf Art, Eingangszeitpunkt, Absender, Adressat etc. zu erfassen und über einen festgelegten Geschäftsgang in der Behörde zu verteilen sowie Ausgänge gemäß der Vorgaben der Sachbearbeitung zu versenden. Diese Aufgaben sind grundsätzlich auch bei der Organisation elektronischer Ein- und Ausgänge in einer E-Poststelle zu erfüllen[15].

Vor diesem Hintergrund lassen sich die im Folgenden dargestellten fachlichen Anforderungen[16] an eine E-Poststelle ableiten[17]. Sie bilden zusammen mit den rechtlichen Anforderungen die Grundlage für die Definition der notwendigen Funktionalitäten, die im Kapitel 2.4 beschrieben sind.

Bei der Einrichtung des elektronischen Zugangs (vgl. Kapitel 2.2.3) für eine Behörde sind diese Anforderungen mit Blick auf die spezifische Aufgabe der Behörde zu ergänzen und zu konkretisieren.

Hinweis

Bei der Analyse der Anforderungen muss u. a. betrachtet werden, welcher Schutzbedarf an die Kommunikation der Behörde besteht. Hierfür ist die Methodik des BSI-Standards 100-2[18] zu empfehlen. Danach wird der Schutzbedarf in die Kategorien

- Normaler Schutzbedarf
- Hoher Schutzbedarf und
- Sehr hoher Schutzbedarf

unterteilt. Eine Zuordnung der Kommunikation einer Behörde zu einer bestimmten Kategorie richtet sich nach dem Schaden, der entstehen kann, wenn die festgelegten Sicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit,

Authentizität etc.) verletzt werden. Solche Schadensauswirkungen können wirtschaftliche Schäden, Beeinträchtigung des informationellen Selbstbestimmungsrechts von Bürgerinnen und Bürgern, Beeinträchtigung der persönlichen Unversehrtheit oder auch ein Verstoß gegen Rechtsnormen sein.

Auf Basis des festgestellten Schutzbedarfs ist ein IT-Sicherheitskonzept für die elektronische Poststelle zu erstellen und umzusetzen[19]. Dafür stellen die BSI-Standards 100-1 bis 100-3 und die IT-Grundschutz-Kataloge eine Vorgehensweise sowie Maßnahmen zur Verfügung[20]. Des Weiteren stellt die Technische Richtlinie des BSI TR-03107 „Elektronische Identitäten und Vertrauensdienste im E-Government“ Kriterien zur Verfügung mit dem Ziel, Verfahren zu elektronischen Identitäten und Vertrauensdiensten für verschiedene Prozesse des E-Government zu bewerten und Vertrauensniveaus zuzuordnen[21].

15 Vgl. BMI, Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Akte, Kapitel 3.2, Berlin, Mai 2012

16 D. h. Was muss eine E-Poststelle leisten können?

17 Vgl. BMI, Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Akte, Kapitel 2.3

18 Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise.

19 Dies ist nicht zwingend als separates Dokument zu erstellen. Wichtig ist vielmehr, geeignete und mit dem IT-Sicherheitsmanagement abgestimmte Maßnahmen für diesen Themenbereich zu definieren und umzusetzen.

20 Vgl. BSI, IT-Grundschutz-Kataloge – Glossar und Begriffsdefinitionen, Stand: 13. EL Stand 2013.

21 BSI TR-03107-1 betrachtet und kategorisiert Mechanismen für elektronische Verwaltungsprozesse zwischen Bürgerinnen/Bürgern/juristischen Personen und Behörden. BSI TR-03107-2 spezifiziert den Schriftformersatz mit elektronischem Identitätsnachweis gemäß VwVfG §3a (2). Er richtet sich somit insbesondere an Behörden, die bestehende analoge und digitale Prozesse zur Abgabe einer Erklärung durch den Bürger ergänzen oder ablösen wollen.

2.3.1 Authentizität und Integrität

Authentizität

Mit dem Begriff „Authentizität“ wird die Eigenschaft bezeichnet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird verwendet, um die Identität von Personen, aber auch von IT-Komponenten oder Anwendungen zu prüfen.

Integrität

Integrität bezeichnet die Korrektheit (Unversehrtheit) von Daten und die korrekte Funktionsweise von Systemen. Für Daten bedeutet Integrität, dass diese vollständig und unverändert sind. In der Informationstechnik wird der Begriff in der Regel weiter gefasst und auf Informationen angewendet. Der Begriff „Information“ bezeichnet Daten, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden[22].

Für eine E-Poststelle muss die Möglichkeit bestehen, bei der Übermittlung von elektronischen Daten die Integrität und die Authentizität der Kommunikationspartner zu prüfen. Im Wesentlichen bedeutet dies, dass Dokumente und Daten inhaltlich unverändert übertragen und ungewünschte Modifikationen[23] erkannt werden sowie Absender ermittelt werden können.

In Fällen mit geringerem Schutzbedarf (z. B. Austausch von allgemeinen Verwaltungsinformationen zwischen Behörden oder allgemeine Anfragen durch Bürgerinnen und Bürger) kann eine einfache E-Mail-Kommunikation erfolgen. Dabei werden Authentizität und Integrität der Daten oft indirekt sichergestellt, da sich die Kommunikationspartner entweder kennen und sie die Richtigkeit der Dokumente und Daten bewerten können oder der Schutzbedarf der Kommunikation keine aufwändigeren Maßnahmen zur Sicherstellung der Authentizität und Integrität der Daten für die Arbeit der Behörde erfordert.

In den Fällen, in denen eine bestimmte Form vorgeschrieben ist bzw. in denen der Schutzbedarf der übermittelten Daten bzw. der Kommunikation in Bezug auf ihre Authentizität und Integrität als mindestens „hoch“ eingestuft wird, besteht die Möglichkeit, diese über geeignete Mechanismen (z. B. Nutzung von Signaturen, Authentifizierung z. B. mithilfe des neuen Personalausweises, De-Mail etc.) abzusichern.

2.3.2 Vollständigkeit und Nachvollziehbarkeit

Vollständigkeit

Im Rahmen der elektronischen Kommunikation bedeutet Vollständigkeit, dass alle Daten (z. B. Dokumente, Metadaten usw.) an die geplanten Empfänger weitergeleitet wurden, die auch weitergeleitet werden sollten. Das bedeutet, dass bei der Übertragung der Daten der Zusammenhang der Datenobjekte nicht verändert wurde[24].

Nachvollziehbarkeit

Unter der Nachvollziehbarkeit versteht man, dass alle wesentlichen Schritte einer Posteingangs- oder -ausgangsbearbeitung von einer unabhängigen Stelle überprüft werden können[25].

Bei der Übermittlung von Nachrichten an eine Behörde oder von einer Behörde ist es zur Wahrung der Vollständigkeit und Nachvollziehbarkeit in vielen Fällen von Bedeutung, wann eine Kommunikation stattgefunden hat und welche Daten bzw. Dokumente übermittelt wurden. Dies ist beispielsweise bei der Wahrung oder Initiierung von Fristen der Fall[26]. Besonders zu beachten ist dies, wenn Dokumente zugestellt werden müssen (vgl. hierzu Kapitel 2.2.4).

Hierfür ist es u. a nötig, den Eingang bzw. den Versand der zu betrachtenden Daten bzw. Dokumente (verbindlich) bestimmen und prüfen bzw. nachweisen zu können. Dies

22 Vgl. BSI, IT-Grundschutz-Kataloge – Glossar und Begriffsdefinitionen, Stand: 11. EL Stand 2009.

23 z. B. auch Veränderung der übertragenen Daten durch Schadsoftware (Viren)

24 Vgl. BSI, Technische Richtlinie 03138, Ersetzendes Scannen, Stand: 20.03.13.

25 Vgl. BSI, Technische Richtlinie 03138, Ersetzendes Scannen, Stand: 20.03.13.

26 z. B. Übermittlung von Antragsunterlagen, Angeboten oder Bescheiden mit Anlagen.

bedeutet in der Regel, den Versand bzw. den Eingang einer Nachricht in einem elektronischen Posteingangs- bzw. Postausgangsbuch[27] oder auch den Empfang einer Nachricht mit einem Zeitstempel[28] zu dokumentieren bzw. die Übermittlung zu einer bestimmten Zeit zu bestätigen.

Je nach Anforderung kann es unterschiedliche Formen der Dokumentation bzw. Bestätigung geben. In einfachen Fällen kann eine (ggf. automatisch erstellte) Empfangsbestätigung ausreichend sein. Ist eine fristgerechte und vollständige Übermittlung der Daten von hoher Bedeutung, kann auch ein qualifizierter Zeitstempel genutzt werden. Bei qualifizierten Zeitstempeln sind vom Aussteller technische Komponenten zu nutzen, die sicherstellen, dass im Zeitstempel die zum Zeitpunkt der Erzeugung gültige gesetzliche Zeit unverfälscht aufgenommen wird (§ 15 (3) SigV) und dass Fälschungen und Verfälschungen ausgeschlossen sind (§ 17 (3) SigG)[29].

Für die E-Poststelle bedeutet dies, dass die eingesetzte E-Poststellen-Infrastruktur für die unterstützten Eingangs- und Ausgangskanäle entsprechende Funktionen für Zeitstempel bzw. die Erstellung von Empfangsbestätigungen zur Verfügung stellen muss bzw. dass Kanäle genutzt werden können, die solche Funktionen bieten (wie De-Mail oder das elektronische Gerichts- und Verwaltungspostfach [EGVP]).

2.3.3 Verfügbarkeit

Verfügbarkeit

Die Verfügbarkeit einer E-Poststelle ist vorhanden, wenn diese von den Anwendern wie vorgesehen genutzt werden kann[30]. Das bedeutet, dass Nachrichten übermittelt bzw. versendet werden können.

Für die Bestimmung der Verfügbarkeitsanforderungen einer E-Poststelle sind ggf. relevante gesetzlich festgelegte Fristen sowie Vorgaben für die Reaktion auf elektronisch zugesandte Informationen zu berücksichtigen.

Während bei Sprechstunden und Telefondienstleistungen eingeschränkte Erreichbarkeiten akzeptiert werden, besteht bei elektronischen Zugängen seitens der Bürgerinnen und Bürger meist die Erwartung, dass eine Behörde rund um die Uhr erreichbar ist. Für die Einrichtung und den Betrieb eines elektronischen Verwaltungszugangs bedeutet dies, dass hohe Anforderungen an die Verfügbarkeit einer E-Poststelle gestellt werden. Dies ist insbesondere dann der Fall, wenn es um die Einhaltung von Fristen geht, an die sich ggf. erhebliche finanzielle Folgen knüpfen können.

Die technische Infrastruktur einer E-Poststelle muss daher eine den spezifischen Anforderungen der Behörde entsprechende Verfügbarkeit ermöglichen. Da die technische Sicherstellung einer hohen Verfügbarkeit kostenintensiv ist, sollte bei der Einrichtung einer E-Poststelle festgelegt werden, in welchem Umfang ein Ausfall einer E-Poststellen-Infrastruktur, d.h. die zeitweise „Nicht-Erreichbarkeit", akzeptabel ist[31].

Wenn die technische Infrastruktur der E-Poststelle ausfällt, sollten die Kommunikationspartner – sofern möglich – über den Ausfall benachrichtigt werden. Dies kann über nicht betroffene Kanäle z. B. über einen Hinweis auf der Webseite geschehen, in der auf den Ausfall der E-Poststellen-Infrastruktur hingewiesen wird.

Neben den technischen Aspekten der Verfügbarkeit und Erreichbarkeit sind auch organisatorische Punkte zu beachten. Bei der Planung der personellen Ausstattung einer Poststelle muss sichergestellt werden, dass genügend ausgebildetes Personal zur Verfügung steht, um eingehende Nachrichten zu sichten und weiterzuleiten bzw. ausgehende Nachrichten zu versenden (vgl. Kapitel 4)[32].

---

27 Da in einem Posteingangs- bzw. Postausgangsbuch unter Umständen personenbezogene Daten enthalten sein können, ist es nötig, den Zugriff nur für berechtigte Nutzerinnen und Nutzern zu ermöglichen.

28 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 Zeitpunkt bei dem Aussteller des Zeitstempels (i. d. R. ein Zertifizierungsdiensteanbieter) vorgelegen haben (S. BSI TR- BSI Technische Richtlinie 03125 „Beweiswerterhaltung kryptografisch signierter Dokumente", Glossar).

29 Vgl. hierzu Anlage 2: Elektronische Signatur

30 Vgl. BSI, IT-Grundschutz-Kataloge, Glossar und Begriffsdefinitionen, 13. EL Stand 2013.

31 Dies hat auch Auswirkungen auf die Ausgestaltung des Systembetriebs. So kann eine hohe Verfügbarkeitsanforderung die Notwendigkeit nach sich ziehen, einen Ausfall des E-Poststellen-Systems auch in der Nacht oder am Wochenende zu beheben.

32 Sollte die E-Poststelle auch für einen Bereich genutzt werden, bei dem Vorgaben zur Erreichbarkeit und Reaktion auf Anfragen einzuhalten sind (sogenannte Servicelevel), dann sind diese bei der Planung der technischen und personellen Verfügbarkeit zu beachten.

2.3.4 Vertraulichkeit und Löschbarkeit

Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein[33]. Dies bedeutet für E-Poststellen, dass Daten und Dokumente vor unzulässiger Einsichtnahme durch Dritte zu schützen sind.

Löschbarkeit

Behörden erhalten in großem Umfang elektronische Post. Teile dieser elektronischen Daten und Dokumente enthalten vertrauliche Informationen, die aus datenschutzrechtlichen Gründen nicht – für Unbefugte zugänglich – in den IT-Systemen der Behörde gespeichert werden sollten (z. B. bei Nichtzuständigkeit). In anderen Fällen muss zur Herstellung einer vollständigen Aktenlage das Löschen von Daten und Dokumenten verhindert werden.

Löschbarkeit beschreibt die Eigenschaft von Daten, mit der festgelegt wird, ob eine Löschung erfolgen darf bzw. muss oder ob diese zu verhindern ist.

Unter Löschen von Daten ist das Unkenntlichmachen der gespeicherten Daten zu verstehen (§ 3(4) Nr. 5 BDSG). Dies ist gegeben, wenn die Daten unwiderruflich so behandelt worden sind, dass eigene Informationen nicht aus gespeicherten Daten gewonnen werden können, wenn also der Rückgriff auf diese Daten nicht mehr möglich ist [ScWi12, § 3 Rn. 75], [Dammann in Simi 11, § 3 Rn. 180][34].

Sofern die Vertraulichkeit der elektronischen Kommunikation, gewährleistet werden muss (z. B. bei personenbezogenen Daten), sind geeignete Maßnahmen zu treffen, um die Daten und Dokumente vor unzulässiger Einsichtnahme durch Dritte zu schützen.

Die Vertraulichkeit der Daten kann durch kryptografische Mechanismen (wie Verschlüsselung des Kommunikationsweges und/oder der Daten) hergestellt werden. Dies soll ermöglichen, dass die zu übertragenden Daten und Dokumente nur durch den/ die ausgewiesene(n) Empfänger/in[35] entschlüsselt und gelesen werden können.

Eine E-Poststelle muss demnach die Möglichkeit bieten, in den Fällen, in denen die zu übermittelnden Daten vertraulich zu behandeln sind, die Übertragung der Daten oder die Daten selbst zu verschlüsseln. Hierfür kann ggf. ein gesonderter Kommunikationskanal angeboten werden.

Bezüglich der Löschbarkeit ist die E-Poststelle der Ort, an dem die Mitarbeiterinnen und Mitarbeiter prüfen müssen, ob eine Löschung vorgenommen bzw. ausgeschlossen werden muss. Ist eine Aufbewahrung nötig, sollten die Daten in zur Aufbewahrung geeignete Systeme (z. B. E-Akte) überführt werden. Dürfen Daten, z. B. aus Gründen des Datenschutzes, nicht aufbewahrt werden, sind diese zu löschen. Dies kann in der Regel nicht pauschal geschehen, sondern es bedarf einer Regelung. Bei einer solchen Regelung ist es zur Vereinfachung der Prüfung sinnvoll, Klassen von Daten zu bilden, in die die Daten gegliedert werden. Für jede Klasse von Daten ist dann festzulegen, ob die Daten aufzubewahren oder zu löschen sind (so sind z. B. Anträge aufzubewahren).

2.3.5 Lesbarkeit und Verkehrsfähigkeit

Lesbarkeit

Lesbarkeit bedeutet, dass die an eine oder von einer Behörde übermittelten Daten bzw. Dokumente entweder von einem Menschen gelesen, verstanden und nachvollzogen, oder aber durch ein IT-System verarbeitet werden können[36].

33 Vgl. BSI, IT-Grundschutz-Kataloge, Glossar und Begriffsdefinitionen, Stand: 13. EL Stand 2013.

34 BSI, Technische Richtlinie 03138, Ersetzendes Scannen, Stand: 20.03.13.

35 Ein ausgewiesener Empfänger kann eine Person, eine Organisationseinheit oder auch eine Behörde sein.

36 Vgl. BSI Technische Richtlinie 03125 - Beweiswerterhaltung kryptografisch signierter Dokumente, Kapitel 4.3.

Verkehrsfähigkeit

Verkehrsfähigkeit bedeutet, dass Dokumente von einem elektronischen System zu einem anderen übertragen werden können, ohne dass die „Qualität" des Dokuments sowie seine Integrität und Authentizität beeinträchtigt werden[37]. Die Verkehrsfähigkeit eines Dokuments ist Voraussetzung für die Vorlage des Dokuments vor Gericht. Als verkehrsfähig gelten elektronische Daten und Dokumente, wenn sie in einem „offen standardisierten und eindeutig interpretierbaren Nutzdatenformat" gespeichert sind[38]. Dadurch wird sichergestellt, dass ausgetauschte Informationen von Kommunikationspartnern ohne großen Aufwand gelesen und weiterverarbeitet werden können[39].

Dies bedeutet, dass bei empfangenen Daten die Lesbarkeit geprüft wird. Dies ist bei der Planung des Eingangsprozesses zu regeln. Bei zu übertragenen Daten und Dokumenten sollten Standardformate bzw. mit dem Kommunikationspartner festgelegte Formate genutzt werden[40].

Kann eine Behörde die übermittelten elektronischen Daten und Dokumente nicht bearbeiten, muss sie dies dem/der Absender/in unverzüglich mitteilen (§ 3a Abs. 3 VwVfG). Um den Prozess der Bearbeitung (insbesondere bei Fristen) nicht unnötig zu beeinträchtigen, sollte daher eine Einschränkung auf bestimmte Datenformate (wie z. B. PDF oder XML) erfolgen. Diese Einschränkungen sollten möglichst zwischen den Kommunikationspartnern abgestimmt werden. Ist dies aufgrund der Masse der Kommunikationspartner nicht möglich, sind diese über die Formateingrenzungen zu informieren (z. B. über die Webseite der Behörde[41]). Dabei sollen möglichst offene Standards bzw. die im SAGA-Modul „Technische Spezifikationen[42]" genannten Formate genutzt werden[43].

Hinweis

Vor dem Hintergrund der Anforderungen an die Langzeitspeicherung kann es sinnvoll sein, als Übertragungsformat Langzeitspeicherformate (wie PDF/A) vorzugeben (z. B. wenn die übertragenen Daten nicht weiter bearbeitet werden müssen). Dies ist z. B. bei der Kommunikation mit einem festen Kreis von Kommunikationspartnern aus Wirtschaft oder Verwaltung denkbar.

Weiterhin sollte bei der Festlegung der Formate darauf geachtet werden, dass die Daten bzw. Dokumente möglichst mit lizenzkostenfreier Software lesbar sind (z. B. PDF). Dies gilt insbesondere für die Daten, die von der Behörde an die Bürgerinnen und Bürger versandt werden.

Für eine E-Poststelle bedeutet dies, dass bei der Übermittlung von Daten eine Formatprüfung geregelt werden muss. Bei empfangenen Daten kann dies entweder manuell oder über technische Prüfroutinen erfolgen. Sind die übermittelten Daten nicht verarbeitungsfähig, so ist die Absenderin oder der Absender gemäß § 3a Abs. 3 VwVfG darauf hinzuweisen. Dies kann beispielsweise über eine automatisch erzeugte E-Mail erfolgen.

Bei der Übermittlung von Informationen ist darauf zu achten, dass die Formatfestlegungen eingehalten werden[44].

37 Vgl. Bundesministerium für Wirtschaft und Energie (BMWi), Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente, Kapitel 3.2

38 Vgl. hierzu: Die Beauftragte der Bundesregierung für Informationstechnik (BfIT), SAGA-Modul Technische Spezifikationen, Version de.bund 5.0.0, 3. November 2011, Kapitel 7

39 Vgl. BSI Technische Richtlinie 03125 - Beweiswerterhaltung kryptografisch signierter Dokumente, Kapitel 4.3.

40 Vgl. auch Kapitel 2.2.3

41 Denkbar ist auch, dass durch die Behörde Vorlagen (z. B. PDF-Formulare) bereitgestellt werden.

42 Vgl. Die Beauftragte der Bundesregierung für Informationstechnik (BfIT), SAGA-Modul Technische Spezifikationen, Version de.bund 5.0.0, 3. November 2011

43 Bei der Kommunikation innerhalb der Bundesverwaltung sind die SAGA-Vorgaben bezüglich zu verwendender technischer Spezifikationen zwingend zu beachten.

44 Auch dies kann durch persönliche oder automatische Prüfung erfolgen. Dabei ist es jedoch nicht nötig, jede Nachricht zu prüfen, da sich die von einer Behörde genutzten Formate i.d.R. nicht fortlaufend ändern.

2.4 Funktionale Anforderungen an eine E-Poststellen-Infrastruktur

In Ergänzung zu den fachlichen Anforderungen wird bei den funktionalen Anforderungen betrachtet, welche Funktionen die technische Infrastruktur einer E-Poststelle bereitstellen sollte, um die fachlichen und rechtlichen Anforderungen zu erfüllen.

Es ist zu beachten, dass es sich bei den folgenden Ausführungen nicht um Funktionen handelt, die alle von einem System zu erfüllen sind. Im einfachsten Fall besteht die E-Poststellen-Infrastruktur aus einem zentralen E-Mail-Postkorb. In komplexeren Fällen werden verschiedene elektronische Kommunikationskanäle und somit verschiedene Systeme genutzt. Dabei können auch Systeme zum Einsatz kommen, mit denen verschiedene elektronische Kommunikationskanäle innerhalb eines Systems gebündelt werden können.

2.4.1 Einbindung verschiedener Kommunikationskanäle

Aufgrund der Unterschiedlichkeit der Kommunikation von Behörden mit externen Partnern sind im Rahmen der Planung und Einrichtung einer E-Poststelle die behördenspezifischen Anforderungen zu analysieren, zu konkretisieren und zu dokumentieren. Je nach Einsatzszenario sind dabei verschiedene elektronische Kommunikationskanäle zu berücksichtigen. Diese können für bestimmte Anwendungsszenarien gesetzlich vorgeschrieben sein.

Unter einem elektronischen Kommunikationskanal versteht man eine Technik, welche zur Übertragung von Nachrichten verwendet wird. Aus heutiger Sicht sind insbesondere die folgenden Kommunikationskanäle zu betrachten.

- **E-Mail**

Die E-Mail ist eine einfache und weit verbreitete Möglichkeit zur elektronischen Kommunikation. Da eine E-Mail allerdings vergleichsweise einfach zu manipulieren ist und es an der Beweisbarkeit von Sende- und Empfangsvorgängen mangelt, ist sie für rechtlich relevante Kommunikation nur bedingt geeignet[45]. Zwar ist es auch per E-Mail möglich, verschlüsselte und signierte Dateien zu versenden, allerdings ist i. d. R. kein automatischer Nachweis der Versendung bzw. des Empfangs gegeben.

- **De-Mail**

In Fällen, in denen Vertraulichkeit, Authentizität, Integrität sowie der Nachweis von Empfang- bzw. Absendevorgängen nötig ist, kann De-Mail genutzt werden (vgl. Kapitel 2.2.5 und Anlage 1).

- **virtuelle Poststelle (VPS)[46]**

Eine virtuelle Poststelle (VPS) ist eine spezielle für die öffentliche Verwaltung entwickelte Form einer elektronischen Poststelle, die eine sichere und nachweisbare Kommunikation ermöglicht (vgl. Kapitel 2.1.). Genau genommen ist eine VPS kein eigenständiger Kommunikationskanal, sondern ein System, in dem bereits verschiedene Kanäle gebündelt werden. Eine besondere Form der VPS ist das Elektronische Gerichts- und Verwaltungspostfach (EGVP).

45 E-Mails sind mit Postkarten vergleichbar, die bei der Übertragung von technisch versierten Dritten gelesen werden können. Sie eignen sich sehr gut zum einfachen und vergleichsweise schnellen Austausch von Informationen. Bei erhöhten Anforderungen an die Sicherheit oder die Nachweisbarkeit sind daher Sicherungsmaßnahmen zu treffen (wie z. B. Verschlüsselung der übermittelten Daten oder Nutzung sicherer Infrastrukturen (wie den Netzen des Bundes) und ggf. automatisch erzeugte Empfangsbestätigungen).

46 Siehe auch Kapitel 2.1

- **elektronische Formulare**

> Über ein im Internet bereitgestelltes editierbares elektronisches Formular ist in der Regel ein medienbruchfreier Austausch von strukturierten Daten und Dokumenten möglich. Dabei werden auf einer Webseite von einem Formularserver bzw. Formularservice[47] Formulare bereitgestellt, die vom Bürger ausgefüllt, ggf. signiert und dann an die Behörde versendet werden. Sollte eine Authentifizierung nötig sein, kann bei Formularen auch die eID-Funktion des neuen Personalausweises genutzt werden. Die Übermittlung der Daten von einem Formularserver bzw. Formularservice an ein Fachverfahren erfolgt meist über eine direkte Fachverfahrensschnittstelle oder als XML-basiertes Datenpaket über eine VPS oder als E-Mail.

Neben den genannten Kanälen sind viele weitere Möglichkeiten denkbar wie z. B. ein direktes Hoch- bzw. Herunterladen von Daten in eine spezielle Ablage, fachverfahrensspezifische Kommunikation zwischen Behörden und ggf. Unternehmen oder aber auch Fax. Eine Nutzung dieser Kanäle kann vor dem Hintergrund fachlicher Anforderungen sinnvoll sein und ist bei der Planung der elektronischen Posteingangs- und -ausgangsbehandlung zu beachten.

2.4.2 Bearbeitung elektronischer Posteingänge

Für eine ordnungsgemäße Behandlung elektronischer Eingänge sollte die E-Poststellen-Infrastruktur folgende Funktionen bereitstellen:

- Die E-Poststellen-Infrastruktur muss es ermöglichen, für jeden unterstützten Kommunikationskanal eine oder mehrere Empfangspostfächer einzurichten.

- Die über einen Kommunikationskanal eingehenden elektronischen Daten und Dokumente an eine Behörde sind durch die E-Poststelle entgegenzunehmen. Dabei soll es möglich sein, den Empfang automatisch zu bestätigen.

- Bei Kommunikationskanälen, über die elektronische Daten und Dokumente übermittelt werden, bei denen der Zeitpunkt des Eingangs wichtig ist (z. B. Nachweis der Fristwahrung bei einem Antragsverfahren) muss es möglich sein, den Eingangszeitpunkt durch das Anbringen eines (ggf. qualifizierten) Zeitstempels zu dokumentieren.

- Darüber hinaus müssen für Kommunikationskanäle, über die elektronische Daten und Dokumente mit hohem oder sehr hohem Schutzbedarf übermittelt werden, entsprechende Funktionen zur Verschlüsselung der Transportwege und ggf. auch der elektronischen Daten und Dokumente zur Verfügung stehen[48].

- Da eine Behörde für den elektronischen Zugang voraussichtlich verschiedene Kommunikationskanäle eröffnen wird, kann es sinnvoll sein, wenn die von der E-Poststelle genutzte Infrastruktur eine konsolidierte Sicht auf die verschiedenen elektronischen Posteingänge ermöglicht. Dabei werden verschiedene Eingangskanäle[49] durch die E-Poststellen-Infrastruktur überwacht bzw. bedient. Eingänge aus verschiedenen Kanälen können in einem Postkorb dargestellt werden und bei Ausgängen ist es aus einem Postkorb heraus möglich, verschiedene Kanäle zu nutzen.

- Weiterhin ist es sinnvoll, dass im Rahmen der E-Poststellen-Infrastruktur Funktionen zum geregelten Import von auf Datenträgern angelieferten Daten bereit gestellt werden. Dies dient der Vereinheitlichung der Abläufe und ist aus Sicherheitsgründen empfehlenswert. Die Nutzung einer solchen Infrastruktur ist bei der Festlegung der Eingangsprozesse zu regeln.

- Bundesbehörden sind auf Grundlage von § 2 Abs. 2 EGovG verpflichtet, den elektronischen Zugang durch De-Mail zu eröffnen[50]. Aus technischer Sicht bedeutet dies, dass entweder die E-Mail-Infrastruktur der Behörde über ein De-Mail-Gateway an den De-Mail-Kommunikationsverbund angeschlossen wird oder ein Webzugang genutzt wird[51].

47 Ein Formularserver bzw.- Formularservice ist ein IT-System, über das elektronische Formulare im Internet bereitgestellt werden können und die Daten an elektronische Verfahren übergeben werden können. Dabei ist es oft möglich, auch Funktionen wie die Übermittlung von Anlagen oder die Signierung von Formularen bereitzustellen.

48 Die Verschlüsselung der Datenübertragung ist in verschiedenen Sicherheitsstufen möglich. Die Anforderungen an den Grad der Verschlüsselung zur Datenübertragung ergeben sich aus dem jeweiligen fachlichen Kontext (Anforderung an Vertraulichkeit und Integrität). Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Kataloge – M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen, Stand: 13. EL Stand 2013 und M 5 Kommunikation Stand: 13. EL Stand 2013

49 Vgl. Kapitel 2.4.1

50 Vgl. Kapitel 2.2.5

51 Vgl. BMI, Grundlagen für den Einsatz von De-Mail in der öffentlichen Verwaltung, V1.0 vom 21. Juni 2012

- Eingehende elektronische Dokumente oder Daten müssen möglichst automatisiert auf Schadsoftware geprüft werden können[52].

- Bei Nachrichten, die in Schriftform eingehen müssen, ist es zum Teil sinnvoll, dass die E-Poststelle prüft, ob die gegebene Formvorschrift eingehalten wurde. Dies gilt insbesondere für Bereiche, in denen bereits im Vorfeld feststeht, dass Posteingänge signiert sein müssen (z. B. bei einem speziellen Eingangskanal für signierte Anträge). In diesen Fällen ist zu prüfen, ob die elektronischen Daten oder Dokumente (qualifiziert) signiert wurden und ob die Signatur gültig ist. Daher müssen von der E-Poststellen-Infrastruktur Funktionen zur Prüfung von Signaturen und zur Dokumentation des Prüfungsergebnisses bereitgestellt werden. Die Dokumentation kann durch ein gesondertes Prüfprotokoll erfolgen, welches der Nachricht angefügt wird[53].

- Bei Daten und Dokumenten, die über den Onlinedienst einer Behörde (z. B. Formularserver) eingehen und bei denen sich die Absenderin oder der Absender authentifizieren muss, kann die eID-Funktion des neuen Personalausweises (nPA) genutzt werden[54]. Falls die eID-Funktion des nPA genutzt werden soll, sollte die Authentizitätsprüfung im Onlinedienst der Behörde erfolgen. In der E-Poststelle wäre allerdings das Authentisierungsergebnis für entsprechende Eingänge zu dokumentieren. Dies ist bei der Einrichtung der Schnittstellen der E-Poststellen-Infrastruktur zu berücksichtigen (z. B. durch Übergabe einer Information, dass die Authentizitätsprüfung erfolgreich war).

- Bei Kommunikationskanälen, auf denen nur bestimmte Formate übertragen werden sollen, sollte eine automatisierte Formatprüfung möglich sein. Bei einem fehlerhaften Prüfergebnis sollte möglichst automatisiert eine Nachricht erzeugt werden, mit der die Absenderin oder der Absender aufgefordert wird, die Nachricht in einem verarbeitungsfähigen Format erneut zu versenden[55].

- Es muss möglich sein, eingehende Nachrichten und ihre Anhänge anzuzeigen. Hierfür sollte eine Ansichtskomponente in die E-Poststellen-Infrastruktur integriert sein[56].

2.4.3 Datenübergabe an andere Systeme

Die in einer E-Poststelle eingehenden elektronischen Daten und Dokumente müssen manuell oder automatisch in ein IT-System (z. B. E-Akte) übergeben werden können. In diesem Zusammenhang stellen sich folgende funktionale Anforderungen:

- Die E-Poststellen-Infrastruktur muss es ermöglichen, Nachrichten und Anlagen[57] an ein anderes IT-System zu übergeben. Dabei muss es möglich sein,

  - nur den Nachrichtentext,

  - nur die Anlage(n),

  - den Nachrichtentext und die Anlage(n) als separate Dokumente oder

  - den Nachrichtentext und die Anlage(n) als ein Gesamtdokument (z. B. E-Maileingang)

  zu übernehmen.

- Darüber hinaus sollen übermittelte strukturierte Daten an IT-Systeme wie z. B. die E-Akte oder ein Fachverfahren übergeben werden können. Die Übernahme soll administrierbar, d.h. anpassbar sein[58].

- Die Übermittlung der Daten sollte auf der Grundlage von Standards (wie z. B. XÖV[59]) erfolgen.

52 Hinweis: Bei der Übermittlung verschlüsselter Daten ist zu berücksichtigen, dass vor einer Prüfung auf Schadsoftware die Daten zu entschlüsseln sind. Das bedeutet, dass in der E-Poststelle entsprechende Systeme und die nötigen Schlüssel zur Verfügung stehen müssen.

53 Falls eine solche Prüfung nur bei einzelnen Dokumenten nötig ist, sollte die Prüfung der Erfüllung der Formerfordernisse im Rahmen der Sachbearbeitung erfolgen. Dabei müssen die nötigen Systeme zur Verfügung stehen.

54 Vgl. hierzu das Personalausweisportal des BMI, http://www.personalausweisportal.de sowie BMI, Der Personalausweis, Anwenderhandbuch für Wirtschaft und Verwaltung.

55 Vgl. auch Kapitel 2.2.4

56 Diese Ansichtskomponente sollte entweder eine leistungsfähige Multiformatkomponente sein oder es wird eine leistungsfähige Komponente zur Formatwandlung integriert, die eingehende Dokumente in ein verarbeitungsfähiges Format wandelt. Bei einer automatisierten Formatwandlung sind Prüfungen der Qualität vorzunehmen, um sicherzustellen, dass das Ergebnis auch verarbeitbar ist.

57 Dies umfasst auch die ggf. erzeugten Prüfprotokolle (z. B. für Signaturen) – Vgl. Anlage 2: „Elektronische Signatur".

58 Vgl. BMI, Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Akte, Kapitel 3.2.1, Berlin, Mai 2012

59 Standards für den elektronischen Datenaustausch innerhalb und mit der öffentlichen Verwaltung, s. www.xoev.de

- Für die Übergabe der Daten in die E-Akte sollte auch eine Übergabe über eine „Content-Management-Interoperability-Services-(CMIS)"-Schnittstelle möglich sein. CMIS ist ein offener internationaler Standard und ermöglicht den produktunabhängigen Zugriff auf unterschiedliche Datenbankbestände von Dokumentenmanagementsystemen[60].

- Bei der Einrichtung von Schnittstellen ist darauf zu achten, dass die datenschutzrechtlichen Vorgaben für den Umgang und die Speicherung von personenbezogenen Daten beachtet werden.

- Des Weiteren ist beim Austausch von Daten auf den direkten schreibenden Zugriff aus bzw. in ein Dokumentenmanagementsystem bzw. Content-Management-System weitestgehend zu verzichten. Der Datenaustausch sollte über definierte Schnittstellen erfolgen. Dies sollte auch berücksichtigt werden, wenn E-Mails in andere Systeme abgelegt oder verschoben werden.

- Beim Einsatz von elektronischen Signaturen und Verschlüsselungsverfahren ist auch die Übergabe der entsprechenden Metadaten und das Vorhalten der Schlüssel für die Entschlüsselung im Verfahren einzuplanen. Bei Einsatz von Signaturen ist die zeitlich begrenzte Gültigkeit dieser zu berücksichtigen[61].

2.4.4 Übernahme von Daten aus IT-Systemen

Die an die Kommunikationspartner einer Behörde zu versendenden Dokumente und Daten werden in der Regel in üblichen Büroanwendungen, der E-Akte, einem Vorgangsbearbeitungssystem, einem Fachfahren oder einem System zur E-Zusammenarbeit erzeugt. Daher muss die E-Poststellen-Infrastruktur folgende Funktionen erfüllen:

- Übernahme von Dokumenten und strukturierten Daten aus IT-Systemen über eine anpassbare XML-basierte Schnittstelle auf der Grundlage von Standards (wie z. B. XDOMEA), soweit die fachlichen Anforderungen dies erfordern.

- Übernahme von Dokumenten und Datenpaketen wie in einem XDOMEA-Paket als Anhang in eine Nachricht[62].

- Darüber hinaus soll die E-Poststellen-Infrastruktur die Möglichkeit bieten, übergebene Dokumente auf Konformität zu vorgegebenen Formaten zu prüfen und ggf. eine Formatwandlung durchzuführen.

2.4.5 Elektronischer Postausgang

Für einen ordnungsgemäßen Versand elektronischer Nachrichten sollte eine E-Poststellen-Infrastruktur folgende Funktionen bereitstellen:

- Beim Versand einer Nachricht sollte es möglich sein, die Nachricht zur Authentifizierung mit einer (ggf. qualifizierten) Signatur zu versehen.

- Die E-Poststellen-Infrastruktur sollte die Möglichkeit bieten, automatisiert einen Absendevermerk[63] zu erstellen. Dieser Absendevermerk soll bei Bedarf an ein IT-System (z. B. E-Akte) übergeben werden können.

- Es sollte möglich sein, den Versendezeitpunkt durch Anbringen eines (ggf. qualifizierten) Zeitstempels am Absendevermerk zu dokumentieren, sofern der Geschäftsprozess es verlangt.

- Darüber hinaus sollten für Kommunikationskanäle, über die Nachrichten mit hohem bzw. sehr hohem Schutzbedarf bzgl. der Vertraulichkeit übermittelt werden, geeignete Funktionen zur Verschlüsselung der Transportwege und ggf. auch der Nachrichten zur Verfügung stehen.

- Da eine Behörde für den elektronischen Zugang voraussichtlich verschiedene Kommunikationskanäle eröffnen wird, ist es sinnvoll, dass die E-Poststellen-Infrastruktur eine konsolidierte Sicht auf verschiedene Ausgangskanäle ermöglicht.

- Die technische Infrastruktur der Poststelle muss zudem Funktionen bereitstellen, die eine förmliche Zustellung im Sinne des Verwaltungszustellungsgesetzes (VwZG) ermöglichen. Dies ist bspw. über De-Mail möglich.

60 Eine XDOMEA-Schnittstelle erlaubt die Übertragung von strukturierten Dokumenten, Vorgängen und Akten auf andere IT-Systeme. CMIS basiert dagegen nicht auf der Logik „Akte, Vorgang und Dokument" sondern legt Dokumente ordnerbasiert in ein Dokumentenmanagementsystem ab.

61 Siehe auch Anlage 2: Elektronische Signatur. „Verfügbarkeit und Prüfbarkeit von Zertifikaten".

62 Ein XDOMEA-Paket kann Dokumente, Vorgänge und Akten sowie Strukturinformationen im XML-Format enthalten. Diese können automatisiert in eine E-Akte, ein Vorgangsbearbeitungssystem oder ein Fachfahren importiert werden.

63 Bei De-Mail enstpricht ein solcher Absendevermerk der „Versandbestätigung", die vom De-Mail-Anbieter des Absenders (auf Wunsch) erstellt wird.

2.5 Nicht-funktionale Anforderungen an eine E-Poststellen-Infrastruktur

Insbesondere aus IT-Sicht sind bei der Planung der Infrastruktur einer E-Poststelle über funktionale und dezidiert fachliche Anforderungen hinaus sind weitere Aspekte zu berücksichtigen. Dies sind z. B.

- **Wartbarkeit**
  Wartbarkeit bedeutet, dass es möglich sein muss, die Komponenten einer E-Poststellen-Infrastruktur einer strukturierten Wartung zu unterziehen (z. B. Einspielen von Updates), ohne dass der Betrieb der E-Poststelle beeinträchtigt wird.

- **Benutzbarkeit**
  Benutzbarkeit bedeutet, dass die Oberflächen der E-Poststellen-Komponenten (sowohl für interne als auch externe Nutzerinnen und Nutzer) möglichst verständlich, einfach erlernbar und bedienbar sind[64].

- **Leistungsfähigkeit**
  Leistungsfähigkeit bedeutet u. a., dass das Antwortzeitverhalten der E-Poststellen-Infrastruktur eine strukturierte und zügige Bearbeitung von elektronischen Ein- und Ausgängen ermöglicht.

Neben diesen Punkten sind bei der Einrichtung einer E-Poststellen-Infrastruktur insbesondere die folgenden nicht-funktionalen Anforderungen zu berücksichtigen.

2.5.1 Skalierbarkeit / Erweiterbarkeit

Bei der Einrichtung einer E-Poststellen-Infrastruktur wird oft mit einzelnen Kommunikationskanälen, einzelnen Organisationseinheiten oder speziellen Prozessen begonnen. Nach erfolgreicher Einführung erfolgt dann ein schrittweiser Ausbau. Daher ist es sinnvoll, die E-Poststellen-Infrastruktur so zu gestalten, dass sie möglichst einfach an sich verändernde Bedarfe angepasst werden kann (z. B. Hinzunahme neuer Kommunikationskanäle). In diesem Zusammenhang sind perspektivisch auch weitere Anforderungen zu beachten wie z. B. die Mehrsprachigkeit des öffentlichen Teils der E-Poststellen-Infrastruktur.

2.5.2 Barrierefreiheit

Bei der Einrichtung einer E-Poststellen-Infrastruktur sind auch die Anforderungen an die Barrierefreiheit zu berücksichtigen. Sofern ein Teil der E-Poststellen-Infrastruktur im Internet bereitgestellt wird, muss dieser nach der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (BITV) barrierefrei umgesetzt sein[65]. Die Anforderungen der Barrierefreiheit stellen ein sehr umfangreiches und sich stetig weiterentwickelndes Themenfeld dar. Bei der Einrichtung der Infrastruktur einer E-Poststelle muss daher eine gesonderte Betrachtung für die jeweiligen konkreten IT-Anwendungen erfolgen, um die jeweiligen Lösungsmöglichkeiten zu berücksichtigen.

2.5.3 Datenschutz

Die über eine E-Poststelle empfangenen oder versandten Daten können personenbezogene Informationen enthalten, die nicht gespeichert werden dürfen bzw. für Unbefugte unzugänglich gespeichert werden müssen. In anderen Fällen ist die Speicherung der Daten nötig, um eine vollständige Aktenlage herzustellen. Ein weiterer Aspekt ist die Auswertung von Nutzungsdaten, die in der Regel unzulässig ist. Für diese Fälle sind organisatorische Regelungen und technische Lösungen zu schaffen, die einen Missbrauch der Daten verhindern oder zumindest erschweren. Aufgrund der Komplexität dieses Themas ist eine konkrete Betrachtung für jede Behörde nötig, um die besonderen Anforderungen zu identifizieren und geeignete Maßnahmen umzusetzen. Die identifizierten Anforderungen an den Datenschutz sowie die zugehörigen Maßnahmen sind in einem mit dem Datenschutzbeauftragten der Behörde abgestimmten Datenschutzkonzept zu dokumentieren.

64 Bei der Gestaltung von Benutzerschnittstellen sollte daher auf gängige Standards geachtet werden.

65 Die BITV regelt die Anforderungen an die Barrierefreiheit für behördliche Internetangebote. Allerdings können entsprechende Anforderungen auch in einer Behörde bestehen, wenn z. B. sehschwache Mitarbeiterinnen und Mitarbeiter mit der E-Poststellen-Infrastruktur arbeiten sollen.

2.6 Weitere Kommunikationsmöglichkeiten zwischen Verwaltung und Externen

Bei der Betrachtung der elektronischen Kommunikation einer Behörde sind neben den „klassischen" Kommunikationskanälen wie E-Mail auch moderne Interaktionsmöglichkeiten zu berücksichtigen. So bieten Techniken wie virtuelle Arbeitsräume, Wikis, Blogs[66], Diskussionsforen[67] oder auch soziale Netzwerke[68] vielfältige Möglichkeiten zur elektronischen Kommunikation mit Bürgerinnen und Bürgern, anderen Behörden oder auch innerhalb einer Behörde. Wie diese Techniken genutzt werden können, wird im Baustein E-Zusammenarbeit beschrieben.

Bei der Nutzung dieser Möglichkeiten durch eine Behörde ist zu beachten, dass eine kontinuierliche Betreuung des jeweiligen Angebotes nötig ist, um aktuelle Informationen bereitzustellen und Anfragen beantworten zu können[69]. Aus Behördensicht werden die o. g. Möglichkeiten meist nur zur allgemeinen Information über die Behörde genutzt. Daher erfolgt die Betreuung meist durch Pressestellen bzw. Webredaktionen und nicht durch E-Poststellen.

Auch ist zu beachten, dass aktenrelevante Informationen – unabhängig vom Kommunikationskanal, mit dem sie ausgetauscht werden – in die elektronische Akte abgelegt werden müssen. Dabei ist zu beachten, dass sie in ein aktenfähiges Format (z. B. PDF/A) überführt werden müssen, um ihre Lesbarkeit zu gewährleisten.

Für Rückmeldungen ist zu prüfen, ob eine Kommunikation über das soziale Netz aus Sicherheits- und Datenschutzerwägung sinnvoll ist oder ob mit dem Adressaten ein alternativer Kommunikationskanal vereinbart wird.

66 Ein Blog steht kurz für „Web-Log(buch)" und ist ein auf einer Webseite geführtes und meist öffentlich einsehbares Tagebuch oder Journal von mindestens einer Person, in dem Aufzeichnungen geführt, Sachverhalte protokolliert, Informationen veröffentlicht oder Gedanken/Meinungen dargestellt werden. Von den Einträgen des Blogs kann auf Dokumente, weiterführende Webseiten usw. verlinkt werden, so dass eine Wissenssammlung zu den verschiedensten Themen entsteht. Eine besondere Form des Bloggens ist das Mikroblogging. Dabei werden nur kurze, SMS-ähnliche Texte veröffentlicht. Vgl. hierzu auch de.wikipedia.org/wiki/Blog (Abruf 22.10.2012) und BMI, Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Zusammenarbeit, Berlin, Mai 2012

67 Ein Diskussionsforum ist eine Webseite, auf der Informationen eingestellt werden (posted messages). Jeder kann neue Informationen einstellen oder auf vorhandene Einträge antworten. (Vgl. BMI, Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Zusammenarbeit, Berlin, Mai 2012 .

68 Ein soziales Netzwerk ist ein meist im Internet verfügbares virtuelles Netzwerk von Menschen oder Organisationen, über das Informationen ausgetauscht werden. Der Zugriff auf soziale Netzwerke erfolgt meist über Webportale, welche Funktionen wie persönliche Profile mit Möglichkeiten zur Anpassung der Sichtbarkeit für verschiedene Mitglieder des Netzes, Adressbücher, Empfang und Versand von Nachrichten (wie Chats, Blogs) etc. bereitstellen. In einem sozialen Netz können die Profile der Nutzer in der Regel beliebig miteinander verknüpft werden, so dass ein gezielter Austausch von Informationen zwischen den verknüpften Personen möglich ist.

69 Bei der Nutzung von sozialen Netzwerken sind die in den IT-Grundschutz-Katalogen unter Punkt M 5.157 „Sichere Nutzung von sozialen Netzwerken" beschriebenen Maßnahmen zu beachten.

3 Umsetzungsszenarien

Die Einrichtung einer E-Poststelle kann sowohl technisch als auch organisatorisch in verschiedenen Strukturen erfolgen. Dabei kann grundsätzlich zwischen zentralen und dezentralen Szenarien unterschieden werden. Im Folgenden wird auf die Vor- und Nachteile der einzelnen Ansätze aus organisatorischer Sicht eingegangen. Die Betrachtung der technischen Lösungsansätze findet sich im Kapitel 3.2.

3.1 Organisatorische Umsetzungsszenarien

Wie in der Einleitung dargestellt, fokussiert dieser Baustein darauf, den Eingang und Ausgang von elektronischen Dokumenten organisatorisch und soweit sinnvoll auch technisch zu regeln. Im Folgenden wird daher auf verschiedene organisatorische Ansätze eingegangen. Welche dieser Ansätze für eine Behörde sinnvoll sind, ist im Rahmen des konkreten Umsetzungsfalls zu erörtern.

3.1.1 Zentrale E-Poststelle

Die für die papierbezogene Eingangsbearbeitung verbreitete zentrale Poststelle und deren Ablauforganisation können auch in der elektronischen Welt abgebildet werden. In diesem Fall wird eine Organisationseinheit mit der Behandlung zentraler elektronischer Posteingänge und -ausgänge beauftragt. Meist wird hierfür die bereits bestehende Poststelle genutzt, die neben der Papierbearbeitung auch die Sichtung der elektronischen Eingänge übernimmt.

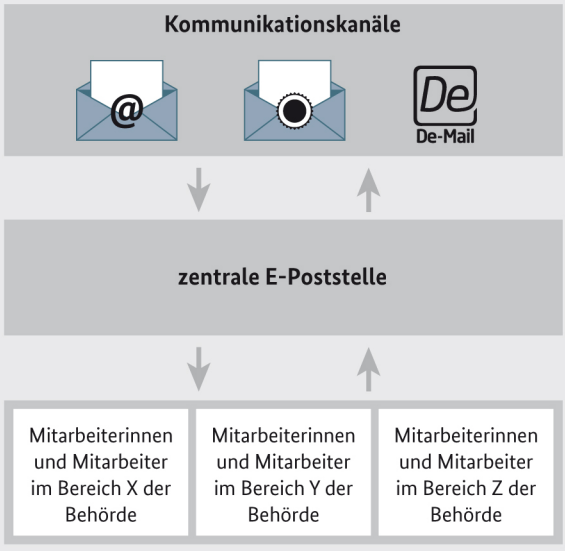


Abbildung 1: vereinfachte organisatorische Darstellung der zentralen E-Poststelle

Für die zentrale Eingangs- und Ausgangsbearbeitung ist festzulegen, welche Kommunikationskanäle von der zentralen E-Poststelle zu überwachen bzw. zu nutzen sind. Zudem sind die Zeiten festzulegen, in denen die Erreichbarkeit und die Bearbeitung durch die Poststelle sichergestellt sein müssen. Die Festlegungen müssen technisch und organisatorisch umgesetzt werden (vgl. Kapitel 3.2). Für den Kanal „E-Mail“ muss z. B. ein zentrales E-Mail-Postfach eingerichtet werden, welches von den Beschäftigten der Poststelle regelmäßig geprüft wird.

Die Vorteile einer zentralen E-Poststelle sind im Wesentlichen die Bereitstellung eines einheitlichen Zugangs für Bürgerinnen und Bürger und eine vergleichsweise effiziente Erfassung der Eingänge, da die Beschäftigten der Poststelle diese Tätigkeit routiniert abwickeln können. Außerdem ist die Erreichbarkeit einer zentralen E-Poststelle durch Vertretungsregelungen einfacher zu sichern als die Erreichbarkeit mehrerer einzelner Mitarbeiterinnen und Mitarbeiter.

Nachteilig kann es bei einer zentralen Poststelle sein, dass dort bei einem hohen Kommunikationsaufkommen Verzögerungen auftreten können, die bei einer dezentralen Ein- und Ausgangsbearbeitung vermieden werden können.

Hinweis:

Wenn für die Poststelle Vorgaben zu Verfügbarkeit und zu Reaktionszeiten bei Anfragen gelten, wie sie z. B. bei der Beantwortung von an die Behörde weitergeleiteten Anfragen aus einem 115-Service-Center gelten (Servicelevel), so sind diese bei der Planung der technischen und der personellen Verfügbarkeit zu berücksichtigen. Dabei sind die Verfügbarkeit und die Servicequalität für zentrale Strukturen i. d. R. leichter sicherzustellen.

3.1.2 Dezentrale E-Poststelle

Bei einer dezentralen Organisation der E-Poststelle können entweder dezentrale Organisationseinheiten oder Bearbeiterinnen und Bearbeiter direkt die Behandlung von Postein- und -ausgängen übernehmen. Bei der direkten Wahrnehmung der E-Poststellenaufgaben durch die Bearbeiterinnen und Bearbeiter sind diese grundsätzlich für die Prüfung und Registrierung sowie den nachvollziehbaren Versand zuständig. Bei der Bearbeitung durch dezentrale Organisationseinheiten ist dort festzulegen, welche Beschäftigten die Sichtung und Prüfung der Eingänge und der Versendung der Ausgänge übernehmen.

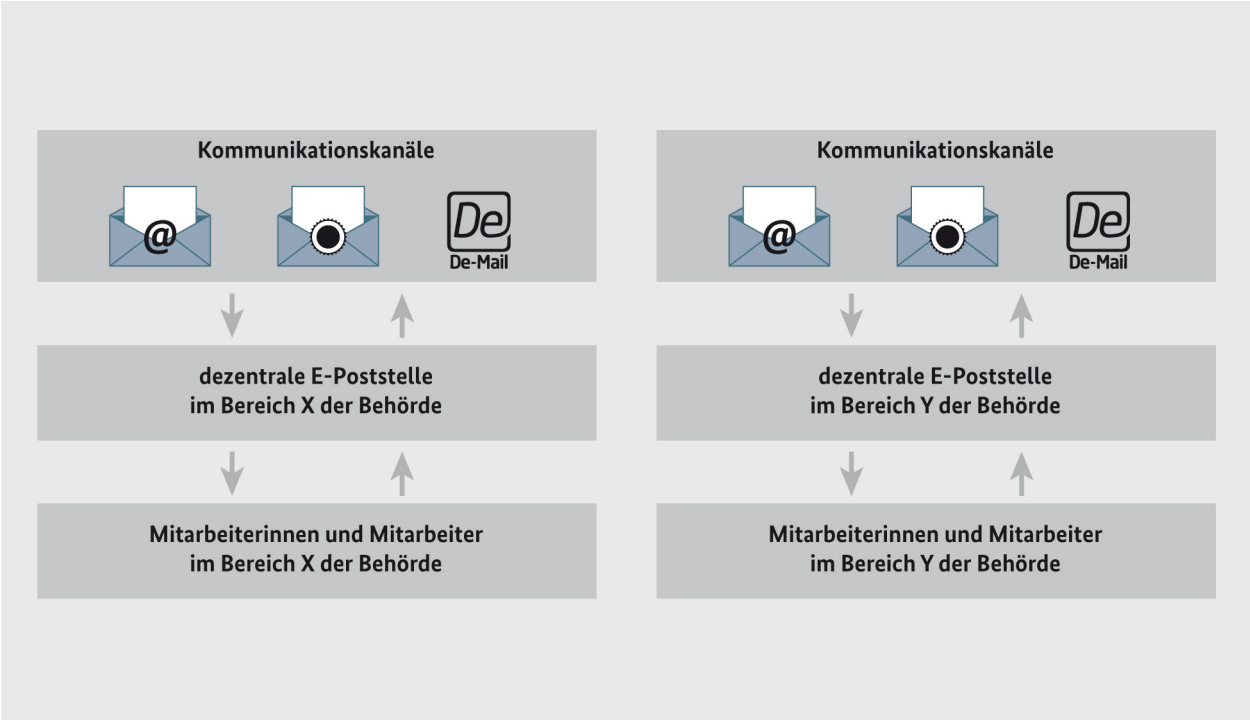


Abbildung 2: vereinfachte organisatorische Darstellung von dezentralen E-Poststelle(n)

Für die Ein- und Ausgangsbehandlung durch die Bearbeiterinnen und Bearbeiter bzw. durch dezentrale E-Poststellen ist festzulegen, welche Eingangskanäle zu überwachen bzw. zu nutzen sind (z.B. Organisations- oder Funktionspostfächer). Zusätzlich sind die notwendigen technischen Möglichkeiten zu schaffen (vgl. Kapitel 3.2).

Die dezentrale Posteingangs- und -ausgangsbehandlung durch Bearbeiterinnen und Bearbeiter wird sich meist auf die Bearbeitung und Versendung von E-Mail-Eingängen beschränken. Allerdings ist es auch denkbar, dass ein Fachverfahren über dezentrale Postkörbe verfügt, welche von den zuständigen Beschäftigten zu prüfen sind.

Eine weitere Möglichkeit ist, dass eine Organisationseinheit aufgabenbezogen, dezentral Poststellenaufgaben wahrnimmt. Das ist der Fall, wenn eine Organisationseinheit ein Fachgebiet verantwortet und elektronische Eingänge zu diesem Gebiet über verschiedene Kanäle eingehen können. Als Beispiel kann hier die Bearbeitung von Förderanträgen genannt werden, bei denen die zuständige Organisationseinheit Anträge über Webformulare in einem Fachverfahren sichten und Statusabfragen über E-Mail oder De-Mail beantworten muss.

Bei dezentralen Eingängen ist zu erwarten, dass sich die Anliegen in den Posteingängen konkret auf das Arbeitsgebiet der Bearbeiterin bzw. des Bearbeiters oder der Organisationseinheit beziehen. Ein Vorteil ist somit, dass Anfragen ohne Zwischenschritte der Sachbearbeitung zur Verfügung stehen. Nachteil kann es sein, dass der Aufwand zur Posteingangsbearbeitung aus Sicht der Gesamtorganisation tendenziell steigt, weil sich viele Stellen in der Behörde mit der Verteilung von Eingängen beschäftigen. Bei der Nutzung von personenbezogenen Postfächern können Verzögerungen durch Personalveränderungen bzw. Krankheits- oder Urlaubsfällen auftreten. Je kleinteiliger die dezentrale E-Poststellenorganisation ist und je höher die Fachspezifika der einzelnen Teams sind, desto schwieriger wird es in der Regel sein, die Erreichbarkeit sicherzustellen.

Weiterhin ist zu beachten, dass dezentrale Posteingänge auch zu einer differenzierten Darstellung einer Behörde nach außen führen. Dies kann für Bürgerinnen und Bürger verwirrend sein und ist kaum mit der Zielsetzung der Schaffung einheitlicher Ansprechpartner zu verbinden.

Hinweis

Bei einer dezentralen Organisation der elektronischen Postbearbeitung ist zu klären, ob personenbezogene Postfächer oder Funktionspostfächer für den Empfang oder das Versenden von Nachrichten genutzt werden sollen. Bei personenbezogenen Postfächern ist zu beachten, dass die Kommunikationspartner wissen müssen, mit welchem Thema sie sich an welche Mitarbeiterin bzw. welchen Mitarbeiter wenden können. Weiterhin ist für den Vertretungsfall zu klären, wer auf die persönlichen Postfächer zugreifen darf, um die kontinuierliche Sachbearbeitung sicherzustellen. Es wird daher empfohlen, neben den personenbezogenen Postfächern Funktionspostfächer einzurichten. Sie bieten einen fachbezogenen elektronischen Verwaltungszugang. Beim Versand über die Funktionspostfächer sollten statt persönlicher Daten die Daten des jeweiligen Funktionspostfaches genutzt werden.

Zusammenfassend ist festzustellen, dass es vom jeweiligen Anwendungsbereich abhängt, ob ein zentraler oder dezentraler Lösungsansatz am besten geeignet ist. Zentrale Strukturen eignen sich insbesondere für Bereiche mit standardisiertem Kommunikationsaufkommen (z. B. Betreuung eines Antragsverfahrens). Für themenbezogene Kommunikationsszenarien, bei denen die Beteiligten wissen, welche Organisationseinheit bzw. welcher Beschäftigter für ihr Thema zuständig ist, ist i.d.R. eine dezentrale Kommunikation sinnvoll. Auch kann es sinnvoll sein, eine Kombination aus zentralen und dezentralen Kommunikationsmöglichkeiten zu wählen, um so den Anforderungen der einzelnen Kommunikationsszenarien optimal entgegenzukommen.

3.2 Technische Umsetzungsszenarien

3.2.1 Zentraler Systemansatz

Im einfachsten Fall einer zentralen E-Poststellen-Infrastruktur wird z. B. ein zentrales E-Mail-Postfach eingerichtet, welches von den Beschäftigten der Poststelle regelmäßig geprüft wird. Dieser Ansatz eines zentralen Postfaches eignet sich meist auch für die Eröffnung des De-Mail-Zugangs einer Behörde (insb. wenn keine besonderen Anwendungsfälle für die Nutzung von De-Mail vorliegen)[70]. Sollen weitere Kommunikationskanäle überwacht werden (wie z. B. VPS), müssen auch für diese Kanäle entsprechende Postfächer eingerichtet werden. Es ist auch möglich, die Eingänge mehrerer Kanäle in einem System zu bündeln[71].

Für den Versand einer Nachricht müsste dann entweder das für den jeweiligen Kanal zur Verfügung stehende IT-System oder aber eine zentralisierte E-Poststellen-Infrastruktur genutzt werden, in der der Kommunikationskanal ausgewählt werden kann.

Unabhängig davon, ob die Verteilung und Bearbeitung der einzelnen Eingangskanäle organisatorisch zentral oder dezentral erfolgt, ist eine technische Bündelung an einem oder wenigen zentralen Punkten erforderlich, um Funktionen wie Virenprüfung, Signaturaufbringung und -prüfung, Ver-/Entschlüsselung, Zeitstempel, ggf. nötige Formatwandlungen etc. zentral bereitzustellen. Dies vereinfacht die Pflege der IT-Infrastruktur und ist insbesondere für die schnelle Umsetzung von zeitkritischen Aktualisierungen von Virenprüfungen, kryptografischen Verfahren und weiteren IT-Sicherheits-maßnahmen erforderlich.

Die technische Bündelung kann mit einem organisatorisch dezentral angelegten Ansatz kombiniert werden, indem die Eingänge nach Durchführung der zentralen Maßnahmen an die dezentralen Organisations- bzw. Funktionspostfächer weitergeleitet werden und die Ausgänge vor der Versendung nach außen über den zentralen Ausgang geleitet werden.

Die folgende Abbildung stellt dies dar:

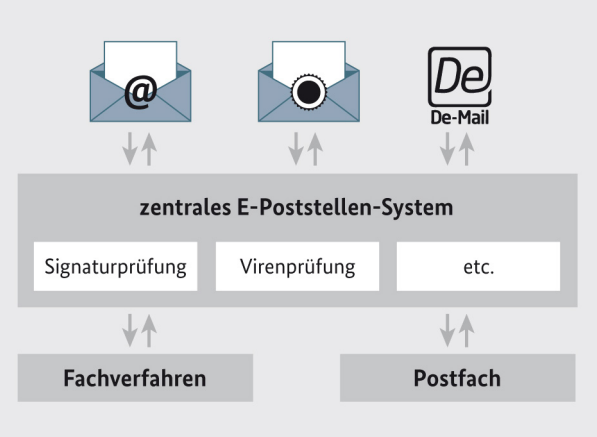


Abbildung 3: vereinfachte Darstellung eines zentralen E-Poststellen-Systems

Die Einrichtung einer zentralen technischen Lösung ist mit erheblichen Vorteilen beim Betrieb und bei der IT-Sicherheit verbunden, so dass i.d.R. der mögliche Aufwand, der bei der Konsolidierung der Ein- und Ausgangspunkte entsteht, aufgrund der späteren Vorteile i.d.R. vertretbar ist. Fall dies jedoch nicht der Fall ist oder aufgrund von übergeordneten Rahmenbedingungen eine Konsolidierung nicht umsetzbar ist, wird ein verteilter Ansatz realisiert.

3.2.2 Verteilter Systemansatz

Eine Alternative zur ggf. technisch aufwendigen Konsolidierung der Posteingangskanäle ist, die einzelnen Kanäle (E-Mail, De-Mail, VPS etc.) getrennt zu überwachen. Somit entsteht zwar kaum technischer Aufwand, allerdings wird die Sicherstellung der erforderlichen Maßnahmen organisatorisch aufwendiger, da gleichzeitig mehrere Systeme zu betreuen sind.

Für den Fall, dass ein verteilter Systemansatz verwendet wird und dennoch für die Bearbeitung von unterschiedlich eingehenden Nachrichten eine zentrale Ablage sinnvoll ist, ist auch denkbar, dass Nachrichten, die über verschiedene Kommunikationskanäle eingehen, aufgrund von speziellen Eigenschaften (Metadaten, bestimmte Adresse etc.) an ein Fachverfahren, eine E-Akte oder einen speziellen Postkorb übergeben werden.[72]

70 Vgl. Anlage 1 – Übersicht De-Mail

71 Dies kann entweder durch die Übergabe der Nachrichten der verschiedenen Kommunikationskanäle an ein zentrales System erfolgen oder aber durch die Versendung einer Notifikations-E-Mail, die auf den Eingang einer Nachricht (z. B. in der VPS) hinweist und möglichst eine Verknüpfung zur Eingangsnachricht enthält.

72 Diese Übergabe lässt sich beispielsweise durch ein Routing bzw. Dispatching von Daten/ Nachrichten auf der Basis von Metadaten realisieren.

3.3 Zusammenspiel technischer und organisatorischer Ansatz

Bei der Planung der elektronischen Eingangsbehandlung und der dafür nötigen technischen Unterstützung ist zu beachten, dass zentrale organisatorische Ansätze sowohl mit zentralen als auch mit verteilten und gemischten technischen Lösungen umgesetzt werden können.

So kann eine zentrale E-Poststelle einen oder mehrere Posteingangskanäle überwachen. Umgekehrt gilt auch, dass zentrale oder verteilte technische Systeme in dezentral organisierten E-Poststellen nutzbar sind.

4 Organisatorische Regelungsbedarfe

Die konkrete Ausgestaltung einer E-Poststelle ist vom fachlichen, organisatorischen und technischen Kontext der Behörde abhängig und muss daher in einem behördenspezifischen Konzept geplant werden. In diesem Konzept sind verschiedene organisatorische Festlegungen zu treffen. Im Folgenden wird auf die wesentlichen zu regelnden Punkte eingegangen.

4.1 Festlegung der Organisationsstruktur

In Abhängigkeit der spezifischen Anforderungen einer Behörde ist es sinnvoll, die Bearbeitung der elektronischen Postein- und -ausgänge zentral, dezentral oder in einer Mischform zu organisieren.

Erfahrungsgemäß werden in der Regel Mischformen sinnvoll sein, bei denen eine zentrale Struktur durch themenspezifische dezentrale Strukturen ergänzt wird. Bei Behörden, die eine homogene Aufgabenstruktur haben, ist dabei eher ein zentraler Ansatz sinnvoll und bei Behörden mit heterogener Aufgabenstruktur sind dezentrale Ansätze praktikabel.

4.2 Festlegung der Verantwortlichkeiten

In Abhängigkeit der gewählten Organisationsstruktur ist u. a. festzulegen, welche Aufgaben bei der Bearbeitung der Postein- und -ausgänge erledigt werden müssen und zu regeln, wie und durch wen sie erledigt werden. Dabei sind nicht nur die Aufgaben der Sichtung der Posteingänge und der Versendung der Ausgänge wichtig, sondern es sind alle in dem Zusammenhang anfallenden Aufgaben zu betrachten. Hierbei sind bereits vorhandene Regelungen zu berücksichtigen bzw. zu aktualisieren. Eine besondere Aufgabe ist in diesem Zusammenhang die kritische Prüfung von Schriftformerfordernissen. In vielen Fällen besteht bei genauer Prüfung kein Schriftformerfordernis, so dass keine Notwendigkeit der Übermittlung per absenderbestätigter De-Mail oder der Anbringung einer qualifizierten Signatur besteht, sondern eine einfache De-Mail oder eine E-Mail ausreicht.

Hinweis

Falls bei der Kommunikation einer Behörde Schriftformerfordernisse vorliegen, ist festzulegen, welche Mitarbeiterinnen und Mitarbeiter nach außen die Behörde vertreten sollen und entsprechend mit der Berechtigung zum Versand absenderbestätigter De-Mails oder mit qualifizierten elektronischen Signaturen (qES) ausgestattet werden. Dabei sollte sich die Behörde an den bestehenden Unterschriftenregelungen (z. B. Geschäftsordnung, Dienstanweisungen) orientieren. Weiterhin ist zu berücksichtigen, dass die Arbeitsplätze der Mitarbeiterinnen und Mitarbeiter bei Einsatz von qES mit der erforderlichen technischen Infrastruktur ausgestattet werden müssen. Dazu zählen unter anderem ein Kartenlesegerät, die Signaturkarte und geeignete Software (z .B. Signaturanwendungskomponente etc.).

Grundsätzlich empfiehlt es sich, die Anzahl der Mitarbeiterinnen und Mitarbeiter, die eine entsprechende Ausstattung zur Nutzung der qES erhalten, zu begrenzen und zentrale Stellen zur Ausstellung von Signaturen einzurichten (z. B. zentrale Poststelle). Allerdings ist dies vor dem Hintergrund der spezifischen fachlichen und rechtlichen Anforderungen kritisch zu prüfen.

4.3 Festlegung der Abläufe

Ergänzend zur Organisationsstruktur sind auch die Abläufe zur Bearbeitung der elektronischen Postein- und -ausgänge festzulegen. Dabei sind die in der Behörde festgelegten Regelungen (z.B. Geschäftsordnung, Hausanordnung) zur Posteingangs- und -ausgangsbehandlung zu berücksichtigen[73].

Bei der Festlegung eines Ablaufs sollte geprüft werden, ob und wie dieser automatisiert werden kann.

Hinweis

Bei der Regelung des Postausgangs sollte überlegt werden, an welcher Stelle ein zentraler Versand (z. B. Rundschreiben) oder ob zur Verringerung von Durchlauf- und Liegezeiten ein dezentraler Versand sinnvoll ist.

4.4 Ermittlung des Personalbedarfes

Bei der Planung einer E-Poststelle sind die Anforderungen an die Verfügbarkeit der E-Poststelle abzustimmen. Diese haben Auswirkungen auf die technische Infrastruktur und das nötige Personal für die Bearbeitung der Ein- und Ausgänge sowie für den Betrieb der technischen Infrastruktur. Möchte eine Behörde die Verfügbarkeit einer Poststelle personell sicherstellen, so ist der erforderliche Personalbedarf in qualitativer, quantitativer, zeitlicher und räumlicher Hinsicht zu bestimmen.

Die qualitative Personalbedarfsermittlung konkretisiert, über welche Qualifikationen das Personal zukünftig verfügen muss. Die quantitative Personalbedarfsermittlung ermittelt die Zahl der für die verschiedenen Aufgaben benötigten Mitarbeiterinnen und Mitarbeiter. Dabei ist zu berücksichtigen, welche Servicezeiten durch die E-Poststelle abgedeckt werden sollen und an welchen Standorten die Mitarbeiterinnen und Mitarbeiter in dieser Zeit zur Verfügung stehen müssen. Weiterhin ist es wichtig, neben dem konkreten Bedarf[74] auch Vertretungsfälle zu regeln, um die Verfügbarkeit dauerhaft gewährleisten zu können[75].

In dem Fall, dass die Anforderungen an die Verfügbarkeit der E-Poststelle einen Schichtbetrieb erforderlich machen, ist dies bei der Ermittlung des Personalbedarfs mit zu berücksichtigen.

4.5 Anpassung von Regelwerken

Bei der Gestaltung der Bearbeitung elektronischer Postein- und -ausgänge müssen die getroffenen Regelungen in einer Dienstanweisung bzw. einer Hausanordnung, ggf. als Anhang (z. B. E-Mail-Regelungen) festgeschrieben werden. Die folgende Tabelle zeigt, welche Themen mindestens berücksichtigt werden sollten[76].

73 Vgl. BMI, Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Akte, Berlin, Mai 2012

74 In Stellen oder Vollzeitäquivalenten

75 Vgl. BMI, Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung http://www.orghandbuch.de/nn_414836/OrganisationsHandbuch/DE/5__Personalbedarfsermittlung/personalbedarfsermittlung-node.html?__nnn=true, Kapitel 5, Stand: Mai 2013

76 Vgl. BMI, Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Akte, Kapitel 3.2.1.3 und Kapitel 3.4.1.2, Berlin, Mai 2012

Regelwerk	Erläuterung
Hausanordnung, Dienstanweisung oder Geschäftsordnung etc.	• Festlegung einer organisatorischen Struktur für die elektronische Eingangs- und Ausgangsbehandlung (zentral/dezentral) • Festlegung von Abläufen und Verantwortlichkeiten (z. B. Eingangsbestätigungen, Rückmeldung bei Nichtverarbeitungsfähigkeit, etc.) • Vorgaben zur Einhaltung von Datenschutz und Datensicherheit sowie zum Umgang mit vertraulichen Eingängen • Erstellung einer behördenspezifischen verbindlichen Positivliste, welche Posteingänge dem Schriftformerfordernis unterliegen bzw. bei welchen die elektronische Form ausgeschlossen ist • Festlegung, wie mit Eingängen zu verfahren ist, die diesen Anforderungen nicht entsprechen • Verpflichtung zur regelmäßigen Prüfung der elektronischen Eingangskanäle • Mit Hinblick auf Bürgerfreundlichkeit und Serviceorientierung kann auch eine Vorgabe von Antwortfristen erfolgen.[77] • Festlegungen zum Umgang mit Schriftformerfordernissen bei Postausgängen - Wer soll im Namen der Behörde absenderbestätigte De-Mails versenden und/oder qualifiziert signieren? - Was soll im Zertifikat der elektronischen Signatur enthalten sein (Name, Pseudonym, Behördenbezeichnung, Zeichnungsberechtigung etc.)? • Sicherstellung der Authentifizierung über elektronische Mechanismen und Etablierung eines verwaltungsintern möglichst weitgehenden Verzichts auf die eigenhändige Unterschrift.
E-Mail-Richtlinie	• Festlegung der nach außen bekanntzugebenden Zugangsdaten (z. B. zentrale E-Mail-Adressen etc.) • Festlegung der ausschließlich dienstlichen Nutzung des E-Mail-Postfachs, insbesondere bei Postfächern der Bearbeiterinnen und Bearbeiter • Umgang mit elektronischen Posteingängen, die offensichtlich Spam

Tabelle 1: Regelungsbedarf Posteingang

4.6 Betreuung von Kommunikationsplattformen

Falls eine Behörde auch eine Kommunikationsplattform betreut (wie z. B. ein soziales Netzwerk), so ist neben der Behandlung der elektronischen Postein- und -ausgänge auch zu regeln, wer die redaktionelle Betreuung der Kommunikationsplattform und der dort betriebenen Blogs und Chats etc. übernimmt. Dabei ist festzulegen, wer zu prüfen hat, ob auf der betreuten Kommunikationsplattform aktenrelevante Daten entstehen und wie diese Daten in die E-Akte überführt werden (z. B. als PDF-Datei).

77 Beispiel ist hier die Behördennummer 115, bei der zu Anfragen, die nicht telefonisch beantwortet werden konnten, innerhalb von 24 Stunden der Servicezeit eine Rückmeldung erfolgen soll.

5 Verknüpfung mit anderen Bausteinen elektronischer Verwaltungsarbeit

Zur elektronischen Aktenführung der eingehenden Dokumente ist die Verknüpfung mit dem Baustein „E-Akte“ notwendig. Dieser deckt die notwendigen Funktionen zur elektronischen Schriftgutverwaltung vollständig ab. Da die Prozesse der Eingangs- und Ausgangsbehandlung auch über die E-Vorgangsbearbeitung oder über E-Fachverfahren abgebildet werden können, sind ggf. auch diese Bausteine zu beachten.

Darüber hinaus sind die im Baustein „E-Langzeitspeicherung“ beschriebenen Vorgaben zu Prozessen und Formaten zu beachten, um die Ein- und Ausgänge ordnungsgemäß langzeitspeichern zu können. Auch sollten die Abläufe der elektronischen Eingangsbehandlung mit den Abläufen zur Digitalisierung der Papiereingänge abgestimmt sein, um eine effiziente Eingangsbehandlung zu ermöglichen. Daher sollten auch die Vorgaben des Bausteins „Scannen“ berücksichtigt werden.

Anlage 1: Übersicht De-Mail

Mit De-Mail können elektronische Nachrichten sicher versendet werden. Im Gegensatz zur herkömmlichen E-Mail können bei De-Mail sowohl die Identität der Kommunikationspartner als auch der Versand und der Eingang von De-Mails jederzeit zweifelsfrei nachgewiesen werden. Die Inhalte einer De-Mail können auf ihrem Weg durch das Internet nicht mitgelesen oder verändert werden. Abgesicherte Anmeldeverfahren und Verbindungen zu den De-Mail-Anbietern sorgen ebenso wie verschlüsselte Transportwege zwischen den De-Mail-Anbietern für einen vertraulichen Versand und Empfang von De-Mails. De-Mail erhöht so die Sicherheit der elektronischen Kommunikation im Vergleich zur herkömmlichen E-Mail und hilft, Spam und Phishing zu vermeiden.

Die Mindestanforderungen an den Nachrichtenaustausch über De-Mail und das Verfahren zur Prüfung dieser Mindestanforderungen (die für alle De-Mail-Anbieter in gleicher Weise gelten) sind im De-Mail-Gesetz geregelt.

De-Mail hat für die elektronische Kommunikation von Behörden eine besondere Bedeutung, da mit Inkrafttreten des E-Government-Gesetzes[78] entsprechend § 2 Abs. 2 Bundesbehörden zur Einrichtung eines De-Mail-Kontos verpflichtet sind. Bei den meisten Erklärungen ist zu erwarten, dass die ggf. nötige Schriftform durch eine Übermittlung der Erklärung über De-Mail ersetzt werden kann.

De-Mail Postfach- und Versanddienst

Die zuverlässige und vertrauliche Kommunikation wird bei der Nutzung von De-Mail über den De-Mail-Postfach- und Versanddienst sichergestellt. Dieser umfasst Funktionen zur Gewährleistung der Vertraulichkeit sowie zum Schutz vor ungewollten Veränderungen des Nachrichteninhaltes und der zugehörigen Metadaten. Dabei stehen vier verschiedene Optionen zur Nachrichtenübermittlung zur Verfügung:

1) Persönlich

2) Absenderbestätigt

3) Versandbestätigung

4) Eingangsbestätigung

5) Abholbestätigung (nur für Behörden)[79].

De-Mail-Zugangseröffnung

Zur wirksamen Zugangseröffnung bedarf es der Erfüllung objektiver und subjektiver Voraussetzungen. Objektive Voraussetzung ist die Bereitstellung einer technischen Infrastruktur für den Empfang und den Versand von elektronischen Dokumenten. Subjektive Voraussetzung ist die Erklärung durch den jeweiligen Kommunikationspartner, dass und wie weit die technische Einrichtung als Zugang dienen soll. Bei der Einrichtung einer E-Poststelle müssen zur Nutzung von De-Mail die im Folgenden aufgeführten Voraussetzungen erfüllt sein.

Schaffung der technischen Infrastruktur

Auf die De-Mail kann auf zwei verschiedenen Wegen zugegriffen werden. Zum einen besteht die Möglichkeit, über ein Web-Portal auf De-Mail zuzugreifen. In diesem Fall muss grundsätzlich keine Erweiterung der bestehenden E-Poststellen-Infrastruktur erfolgen. Komfortabler ist allerdings die direkte Anbindung der bestehenden IT-Infrastruktur über ein De-Mail-Gateway. Diese Variante ermöglicht den direkten Empfang und Versand von De-Mails aus dem E-Mail-System oder einem Fachverfahren heraus. In diesem Fall ist eine Erweiterung der bestehenden E-Poststellen-Infrastruktur um die Anbindung an das De-Mail-Gateway (z. B. das zentral für die Bundesverwaltung betriebene) vorzunehmen[80].

Neben der Schaffung dieser grundlegenden technischen Voraussetzungen für die Nutzung von De-Mail holt der akkreditierte Diensteanbieter zur Sicherstellung der Identität der öffentlichen Stelle und ihrer gesetzlichen Vertreter verschiedene Angaben von der Behörde ein. Dies

78 Vgl. Kapitel 2.2.5

79 Eine detaillierte Beschreibung der verschiedenen Versandoptionen findet sich unter: BSI, De-Mail – eine Infrastruktur für sichere Kommunikation, www.bsi.bund.de/DE/Themen/EGovernment/DeMail/DeMail_node.html (Abruf 22.10.2012)

80 Eine ausführliche Beschreibung der unterschiedlichen Zugriffsmöglichkeiten sowie der technischen Anforderungen hinsichtlich der Anbindung der Behördeninfrastruktur an das De-Mail-Gateway findet sich unter: Bundesministerium des Innern (BMI), Grundlagen für den Einsatz von De-Mail in der öffentlichen Verwaltung, Kapitel 3.5

heißt für die Behörde, die zukünftig mit De-Mail arbeiten möchte, dass sie dazu verpflichtet ist, folgende Angaben über die öffentliche Stelle zu geben:

- Name oder Bezeichnung,
- Rechtsform,
- Anschrift des Sitzes oder der Hauptniederlassung,
- Namen der Mitglieder des Vertretungsorgans oder der gesetzlichen Vertreter.

Da der akkreditierte Diensteanbieter laut De-Mail-Gesetz die Angaben vor Freischaltung des De-Mail-Kontos zu überprüfen hat, muss die öffentliche Stelle zur Freischaltung des De-Mail-Kontos ihre Identität nachweisen (z. B. durch die Identifizierung der entsprechend vertretungsberechtigten Personen). Nachdem weitere Formalien geklärt wurden, die im De-Mail-Gesetz geregelt sind, kann die Behörde die Funktionen von De-Mail nutzen.

Der Gesetzgeber hat durch verschiedene Gesetze im Bereich des E-Government und der E-Justiz klargestellt, dass er De-Mail als sicherem Übermittlungsweg einen besonderen Stellenwert einräumt. Mit dem E-Government-Gesetz wurde darüber hinaus klargestellt, dass De-Mail auch im Bereich des Steuer- und Sozialgeheimnisses ohne zusätzliche Sicherheitsmaßnahmen eingesetzt werden kann (Begründung zu Artikel 2 EGovG). Abweichend von diesem Grundsatz kann es Ausnahmen geben, bei denen im Einzelfall aufgrund eines besonders hohen Schutzbedarfs zusätzliche Sicherheitsmaßnahmen (wie Ende-zu-Ende-Verschlüsselung nach Absatz 3 Satz 3 De-Mail-G) erforderlich werden können.

Sollten solche besonders hohen Anforderungen an die Vertraulichkeit der Nachrichten im Einzelfall vorliegen, ist hierfür die Installation zusätzlicher Software erforderlich, die diese zusätzliche Ver- und Entschlüsselung durchführt. Für die De-Mail-Nutzung in der Behörde bedeutet dies, dass geprüft werden muss, ob die externen Kommunikationsprozesse, die über De-Mail abgewickelt werden sollen, einen solchen besonders hohen Schutzbedarf haben. Trifft dies für einzelne Kommunikationsprozesse zu, muss geprüft werden, in welchem Maße die Vertraulichkeit gewährleistet sein muss und ob es dazu der Installation zusätzlicher Softwareprogramme bedarf.

Erklärung des Kommunikationspartners (Widmung)

Nachdem die Behörde sowie die externen Kommunikationspartner den technischen Zugang zu De-Mail geschaffen haben, müssen diese den Zugang eröffnen. Dabei unterliegt die Zugangseröffnung den Bestimmungen des Verwaltungsverfahrensgesetzes (vgl. Abschnitt 2.2.3). Demnach kann die Eröffnung eines Zugangs sowohl durch ausdrückliche Erklärung als auch durch konkludentes Handeln erfolgen.

Die öffentlichen Stellen müssen den Zugang gemäß dem jeweils geltenden Verfahrensgesetz eröffnen. Dies kann z. B. durch die Angabe der De-Mail-Adresse auf der Homepage erfolgen. Es ist zu beachten, dass es Ausnahmen und Sonderregelungen geben kann (z. B. VwVfg des Landes Baden-Württemberg, wonach die Behörde die Eröffnung ausdrücklich erklären muss)[81].

Bei der Einrichtung von De-Mail müssen also die Adressen, sofern keine Spezialregelungen vorliegen, von der Behörde publiziert werden. Dies kann durch Angabe der Adresse auf der Homepage, einer Visitenkarte oder den Briefköpfen der externen Verwaltungsdokumente stattfinden. Damit ist der Zugang seitens der Behörde eröffnet.

Für die Nutzung von De-Mail für die elektronische Abwicklung von Kommunikationsprozessen ist jedoch wichtig, dass auch der jeweilige externe Kommunikationspartner den Zugang eröffnet. Die De-Mail nutzende Behörde muss also beachten, dass der Adressat den Zugang wirksam eröffnet hat.

Juristische und natürliche Personen im Rahmen eines ständigen Geschäftsbetriebes (z. B. Rechtsanwälte) können den Zugang wie öffentliche Einrichtungen ausdrücklich oder konkludent eröffnen. Für alle weiteren natürlichen Personen wird angenommen, dass sie den elektronischen Zugang für die Behördenkommunikation ausdrücklich erklären müssen. In Fachkreisen wird jedoch diskutiert, dass der Zugang auch durch private Personen konkludent eröffnet werden kann, da Nutzer von De-Mail während der Beantragung des De-Mail-Kontos darüber aufgeklärt werden, dass De-Mail eine besonders gesicherte und verbindliche Form der elektronischen Kommunikation ist. Demnach kann unterstellt werden, dass bei Angabe der De-Mail-Adresse im Absender eine Zugangseröffnung erfolgt, wenn dem Schreiben keine ausdrückliche Einschränkung der Nutzung der De-Mail-Adresse entnommen werden kann.

Die Regelungen des E-Government-Gesetzes ermöglichen zudem, dass De-Mail-Nutzer künftig den Zugang über De-Mail durch eine entsprechende zusätzliche Erklärung im De-Mail-Verzeichnisdienst eröffnen können. So muss nach dem durch das EGovG geänderten § 7 De-Mail-G der akkreditierte Diensteanbieter durch einen geeigneten Zusatz die Erklärung des Nutzers im Verzeichnisdienst veröffentlichen, dass dieser den Zugang im Sinne von § 3a des Verwaltungsverfahrensgesetzes, § 36a Absatz 1 des Ersten Buches Sozialgesetzbuch und des § 87a Absatz 1 Satz 1 der Abgabenordnung eröffnen will. Die freiwillige Veröffentlichung der De-Mail-Adresse im De-Mail-Verzeichnis ohne diese zusätzliche Erklärung stellt jedoch keine konkludente Zugangseröffnung dar[82].

Für die Nutzung von De-Mail im Rahmen der E-Poststelle heißt dies, dass die Behörde beachten muss, wer der externe Kommunikationspartner ist (juristische, natürliche Person im Rahmen eines ständigen Geschäftsbetriebes oder eine private Person) und ob von ihm eine ausdrückliche oder konkludente Zugangseröffnung erfolgt ist.

Weiterhin muss die Behörde die Reichweite der Zugangseröffnung berücksichtigen. Denn natürliche Personen sind verpflichtet, in der Kommunikation mit der Verwaltung zu entscheiden, ob sie ihren Zugang einzelfallbezogen oder generell eröffnen. Allgemein gilt die Zugangseröffnung, wenn nichts anderes ausdrücklich erklärt oder zweifelsfrei erkennbar ist, nur für den jeweiligen Einzelfall. Zu einer generellen Zugangseröffnung müsste die De-Mail-Adresse von der Behörde wie eine Adressangabe aktenkundig gemacht werden. Die generelle Zugangseröffnung würde dann für diese Behörde gelten.

Zusammenfassend ist festzuhalten, dass sowohl die Behörde als auch der externe Kommunikationspartner den Zugang wirksam eröffnen muss. Zur Nutzung von De-Mail muss die Behörde folgende Aspekte beachten:

- Berücksichtigung eventueller Spezialregelungen zur Zugangseröffnung der Behörde
- Publikation der De-Mail-Adresse über die ihr zur Verfügung stehenden Kanäle (bzw. ausdrückliche Erklärung der Zugangseröffnung)
- Prüfen der wirksamen Zugangseröffnung (inkl. Reichweite) des Kommunikationspartners

Weiterhin sollte bei der Integration von De-Mail durch die Behörde geprüft werden, bei welchen Prozessen weitere spezielle Anforderungen an die Zugangseröffnung und die Erfüllung von Formerfordernissen im jeweiligen Einzelfall bestehen. Die Anforderungen können je nach Beteiligten und Zweck des Kommunikationsvorgangs abweichen.

Einführung von De-Mail

Neben der Schaffung der subjektiven und objektiven Voraussetzungen zur Nutzung von De-Mail sollte die Behörde die Einführung von De-Mail detailliert planen. Das Kompetenzzentrum De-Mail hat dazu einen Leitfaden zur Einführung von De-Mail entwickelt[83]. Dieser Leitfaden sieht vor, dass eine Machbarkeitsstudie und eine Wirtschaftlichkeitsbetrachtung vorgenommen, ein Fachkonzept angefertigt und eine Realisierungsplanung erstellt werden sollen.

Im Rahmen der Machbarkeitsstudie sollen die relevanten Prozesse identifiziert, dokumentiert und analysiert werden. Die Analyse der Machbarkeit soll dabei in Hinblick auf die De-Mail-Eignung der Prozesse in rechtlicher, fachlicher und technischer Hinsicht stattfinden.

Ziel der Wirtschaftlichkeitsbetrachtung ist die Ermittlung der monetären Kosten, des Nutzens und der qualitativen Nutzenaspekte. Dazu sollen Kosten und Nutzen anhand vorliegender Fallzahlen, Rahmenbedingungen und erwarteter Nutzungszahlen betrachtet werden.

Im Fachkonzept sollen die Prozesse modelliert werden, die mittels De-Mail abgewickelt werden sollen. In diesem Zusammenhang ist festzulegen, welche konkreten Postfächer bzw. Funktionspostfächer eingerichtet werden sollen und wie und durch wen die Eingangs- und Ausgangsbehandlung erfolgen soll (siehe Kapitel 3). Dies kann beispielsweise durch berechtigte Nutzer direkt in einem De-Mail-Postfach der Behörde erfolgen oder durch Integration von De-Mail in die E-Poststellen-Infrastruktur[84]. Weiterhin sind ggf. Regelungen zur elektronischen Aktenführung von De-Mails zu schaffen und in der Geschäftsordnung zu hinterlegen. Dabei ist insbesondere zu klären, wann und durch wen bei einer signierten De-Mail eine Signaturprüfung erfolgt und wann, durch wen und über welches Verfahren eine Wandlung der Dokumente und Protokollinformationen in das Langzeitspeicherformat PDF/A erfolgt[85].

82 Vgl. BMI, Grundlagen für den Einsatz von De-Mail in der öffentlichen Verwaltung, Kapitel 2.2

83 Vgl. BMI: Grundlagen für den Einsatz von De-Mail in der öffentlichen Verwaltung, Kapitel 3

84 Vgl. Kapitel 3.2

85 Siehe hierzu „Grundlagen für den Einsatz von De-Mail in der öffentlichen Verwaltung“, Publikation BMI, Juni 2012

Darüber hinaus sollen die ggf. existierenden Anforderungen an Schnittstellen und die Übergabe von Nachrichten erläutert werden. Abschließend sollen bei der Realisierungsplanung die strategische Umsetzung/Einführung beschrieben und die Projekt- und Meilensteinpläne, Umsetzungschecklisten und Vergabevorschläge definiert werden[86].

Hinweis

Wie im Kapitel 3 „Umsetzungsszenarien“ dargestellt, gibt es verschiedene Möglichkeiten zur Gestaltung einer E-Poststelle. Die konkrete Ausgestaltung ist vom fachlichen, organisatorischen und technischen Kontext der Behörde abhängig. So kann die Nutzung verschiedener Kommunikationskanäle notwendig sein, um die fachlichen und organisatorischen Anforderungen zu erfüllen. Daher ist es sinnvoll, bei der Einführung von De-Mail nicht nur eine auf De-Mail fokussierte Konzeption vorzunehmen, sondern ein übergreifendes Konzept für die elektronische Kommunikation zu erstellen.

Einsatzszenarien von De-Mail

Bei der Einführung von De-Mail müssen von der Behörde zu Beginn die möglichen Einsatzszenarien von De-Mail geprüft werden (z. B. Nutzung in einem Antragsverfahren oder zur allgemeinen Kommunikation).

Die elektronische Abwicklung externer Kommunikationsbeziehungen per De-Mail kann je nach Bedarf der Behörde unterschiedlich ausgestaltet werden. Demnach ergeben sich verschiedene Einsatzszenarien für De-Mail. Das Kompetenzzentrum De-Mail für die Öffentliche Verwaltung hat die unterschiedlichen Einsatzszenarien in „De-Mail-Einsatzszenarien“ (V 1.0 vom 21. Juni 2012) aufbereitet. In diesem Dokument werden die Möglichkeiten der De-Mail-Nutzung aufgezeigt und der Nutzen sowie die Kostenbestandteile beschrieben.

86 Ausführliche Angaben zu den einzelnen konzeptionellen Modulen einer De-Mail-Einführung können dem Dokument „Grundlagen für den Einsatz von De-Mail in der öffentlichen Verwaltung“ (V 1.0 vom 21. Juni 2012) entnommen werden.

Anlage 2: Elektronische Signatur

Rechtlicher Rahmen

Der rechtliche Rahmen der elektronischen Signatur in Deutschland ist durch das Signaturgesetz (SigG) und die Signaturverordnung (SigV) definiert. Diese Signaturgesetzgebung ist vor dem Hintergrund der EU-Richtlinie (1999/93/EG) für elektronische Signaturen und im Kontext weiterer nationaler Rechtsvorschriften zu sehen, die den Einsatz elektronischer Signaturen im Rechtsverkehr regeln[87]. Darüber hinaus wurden vom Gesetzgeber verschiedene Gesetze so angepasst, dass die Nutzung elektronischer Signaturen in Geschäfts- und Verwaltungsprozessen möglich, zum Teil sogar vorgeschrieben ist (z. B. ZPO, VwVfG, Emissionshandelsgesetz).

Bedeutung der elektronischen Signatur für die elektronische Aktenführung

Vor dem Hintergrund der rechtlichen Rahmenbedingungen ist festzustellen, dass die Nutzung elektronischer Dokumente bis auf wenige Ausnahmen die Nutzung von Papierdokumenten ersetzen kann[88]. Darüber hinaus ermöglichen elektronische Signaturen die Prüfung der Authentizität und der Integrität der Dokumente.

Neben diesem Vorteil bringt der Einsatz elektronischer Signaturen jedoch auch zusätzliche Aufgaben, die im Rahmen der elektronischen Aktenführung zu beachten sind. So muss beispielsweise nach § 17 SigV ein signiertes Dokument (wenn dieses für längere Zeit in signierter Form benötigt wird) übersigniert werden. Signaturen gelten zu einem bestimmten Zeitpunkt als kryptografisch nicht mehr sicher[89]. Ein Ansatz, um dieses Problem zu lösen, ist der Einsatz einer Middleware entsprechend der TR-03125 des BSI[90]. Weitere Ansätze finden sich im Baustein „Langzeitspeicherung“ des Organisationskonzeptes elektronische Verwaltungsarbeit.

Arten der elektronischen Signatur

Nach SigG wird bei der elektronischen Signatur zwischen drei verschiedenen Qualitätsstufen unterschieden:

- [einfachen] elektronischen Signaturen
- fortgeschrittenen elektronischen Signaturen
- qualifizierten elektronischen Signaturen

Im Folgenden werden die einzelnen Signaturarten erklärt.

Abbildung 4 - Arten einer elektronischen Signatur[91]

87 Vgl. BSI, Grundlagen der elektronischen Signatur, Rechtliche Rahmenbedingungen, BSI 2006, Seite 2ff.

88 Vgl. BMI, Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Akte, Kapitel 2.3

89 Als kryptografisch unsicher gelten Signaturen, wenn eine Veränderung und Manipulation des signierten Dokumentes möglich ist, ohne dass die Signatur dabei zerstört wird. Die Bundesnetzagentur gibt regelmäßig in Zusammenarbeit mit dem BSI einen Algorithmenkatalog heraus, der die Sicherheit der aktuell verwendeten Algorithmen für kryptografische Funktionen beschreibt und ein voraussichtliches Ablaufdatum benennt.

90 Technische Richtlinie 03125 (TR-03125) des BSI, s. https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html

91 Vgl. auch BSI, Grundlagen der elektronischen Signatur, Bonn 2006, S. 8

Einfache elektronische Signatur

Die einfache Signatur bezeichnet elektronische Authentifizierungsdaten, die anderen elektronischen Daten beigefügt oder mit ihnen verknüpft sind (vergl. § 2 Nr. 1 SigG). Zur einfachen Signatur zählen auch eingescannte Unterschriften in E-Mails oder am Ende einer E-Mail zugefügte Angaben zur Person, Behörde etc. (Funktion „Signatur" in E-Mail-Programmen). Eine derartige E-Mail-Signatur könnte wie folgt gestaltet sein:

Mit freundlichen Grüßen

Max Mustermann

Referat O1 - Grundsatzangelegenheiten
Bundesministerium des Innern
Alt-Moabit 101 D, 10559 Berlin
Telefon: (030) 18 681 - 2555
Fax: (030) 18 681 - 52555
E-Mail: max.mustermann@bmi.bund.de
Internet: http://www.bmi.bund.de

Abbildung 5: Beispiel für eine einfache elektronische Signatur

Fortgeschrittene elektronische Signatur

Die fortgeschrittene Signatur ist der Signaturschlüsselinhaberin bzw. dem Signaturschlüsselinhaber (Unterzeichnerin bzw. Unterzeichner) zugeordnet und ermöglicht die Identifizierung der Unterzeichnerin oder des Unterzeichners. Sie wird mit Mitteln erstellt, über die nur die Unterzeichnerin oder der Unterzeichner verfügt. Weiterhin ist sie mit den elektronischen Daten so verknüpft, dass eine nachträgliche Änderung der Daten erkennbar ist (vgl. § 2 Nr. 2 SigG). Wird eine fortgeschrittene Signatur als sichtbare Signatur[92] auf einem PDF-Dokument angebracht, könnte sie wie folgt gestaltet sein:

Mit freundlichen Grüßen

Max Mustermann
Datum: 2013.02.10 18:21:07+01'00'

Max Mustermann

Referat O1 - Grundsatzangelegenheiten

Abbildung 6: Beispiel für eine fortgeschrittene Signatur

Es ist auch möglich, ein Bild (wie z. B. eine eingescannte Unterschrift) und weitere Informationen wie z. B. die Organisation oder die Rolle des Unterzeichnenden anzugeben.

Qualifizierte elektronische Signatur

Qualifizierte elektronische Signatur (Zertifikat von einem Zertifizierungsdiensteanbieter (ZDA) mit Betriebsanzeige)

Die qualifizierte elektronische Signatur ist eine besondere Form der fortgeschrittenen elektronischen Signatur. Sie erweitert diese um zwei Punkte. Zum einen muss die Signatur zum Zeitpunkt der Erzeugung auf einem gültigen Zertifikat beruhen, das von einem Zertifizierungsdienstleister[93] nach §§ 4 bis 14 SigG ausgegeben wurde. Zum anderen muss die Signatur durch sog. sichere Signaturerstellungseinheiten[94] erstellt werden (vgl. 2 Nr. 10 SigG)[95].

Diese Signaturerstellungseinheiten stellen Anforderungen an die Fälschungssicherheit und Geheimhaltung von Schlüsseln (§17 SigG), aber auch an die Bedienung der entsprechenden Komponenten durch die Unterzeichnerin und den Unterzeichner. Insbesondere die Notwendigkeit, einen Signaturschlüssel zu besitzen und bewusst anwenden zu können, schließt eine rein softwarebasierte Lösung für die qualifizierte elektronische Signatur aus[96].

Die qualifizierte elektronische Signatur hat im Rechtsgeschäft die gleiche rechtsverbindliche Wirkung wie die eigenhändige Unterschrift, es sei denn, es wird vom Gesetz anders bestimmt. Die Infrastruktur für den Einsatz von

92 Signaturen können sowohl als sichtbare als auch als nicht sichtbare Signaturen angebracht werden. Vgl. Anlage 2: „Anbringungsformen"

93 Zertifizierungsdiensteanbieter sind die in Deutschland tätigen juristischen Personen, die der Bundesnetzagentur gem. § 4 Abs. 3 des Signaturgesetzes i.V.m. §§ 1, 2 der Signaturverordnung das Ausstellen qualifizierter Zertifikate oder qualifizierter Zeitstempel angezeigt haben.

94 Sichere Signaturerstellungseinheiten sind Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, die mindestens die Anforderungen des SigG und der SigV erfüllen und die für qualifizierte elektronische Signaturen bestimmt sind. In Deutschland sind dies in der Regel Prozessor-Chipkarten (Signaturkarten). Es gibt Signaturkarten, mit denen immer nur eine Signatur erzeugt werden kann und Multisignaturkarten, mit denen mehrere Signaturen auf einmal erzeugt werden können.

95 Bei Anbringung als sichtbare Signatur lässt sich eine qualifizierte elektronische Signatur nicht von einer fortgeschrittenen unterscheiden.

96 Daher werden für qualifizierte elektronische Signaturen Signaturkarten benötigt, auf denen das entsprechende Zertifikat gespeichert ist.

qualifizierten elektronischen Signaturen wird über einen Zertifizierungsdiensteanbieter sichergestellt. Die Nutzung der qualifizierten elektronischen Signatur ermöglicht es, zahlreiche Rechtsgeschäfte durchgängig elektronisch durchzuführen. Die in diesem Zusammenhang erstellten Dokumente können somit ohne Medienbruch in der elektronischen Akte abgelegt werden.

Qualifizierte elektronische Signatur (Zertifikat von einem ZDA mit Anbieter-Akkreditierung)

Für die qualifizierte elektronische Signatur wird nach SigG und SigV noch eine Erweiterung vorgesehen, die jedoch keinen technischen Unterschied darstellt. Der Unterschied besteht lediglich darin, dass sich der Zertifizierungsanbieter sein Zertifikat von der Regulierungsbehörde für Telekommunikation und Post beurkunden lässt, welches zur Überprüfung der auszugebenden Zertifikate verwendet wird. Die Signatur muss mindestens 30 Jahre ab dem Jahr überprüfbar sein, in dem das Signaturzertifikat seine Gültigkeit verloren hat (Bei Zertifizierungsdiensteanbietern ohne Anbieter-Akkreditierung genügen fünf Jahre)[97].

Qualifizierte Zeitstempel

Neben den Signaturen sind im SigG auch Regelungen für qualifizierte Zeitstempel enthalten. Qualifizierte Zeitstempel sind elektronische Bescheinigungen eines Zertifizierungsdiensteanbieters, dass ihm bestimmte Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Sie haben eine besondere Bedeutung bei der Übersignierung von Daten, da für die Übersignierung nach § 17 SigV ein qualifizierter Zeitstempel aufgebracht werden muss. Dabei handelt es sich um eine zeitliche Verlängerung der Signatur, wenn die signierten Dokumente „für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind[98]." Zur Ermittlung des Ablaufzeitpunkts wird dann der auf der Signatur angebrachte Zeitstempel herangezogen.

Das Grundprinzip der elektronischen Signatur[99]

Ein wesentlicher Grund für die Schriftform ist, dass alle prüfen können, ob ein Dokument (Urkunde) von einer Person (Unterzeichnerin und Unterzeichner) unterzeichnet wurde. Bei elektronischen Signaturen soll daher die Signatur ausschließlich von der Unterzeichnerin und dem Unterzeichner erzeugt, aber durch alle verifiziert werden können.

Zur Erzeugung elektronischer Signaturen werden sogenannte asymmetrische Verschlüsselungsalgorithmen genutzt, bei denen ein Schlüsselpaar, bestehend aus einem privaten Schlüssel (private key) und einem öffentlichen Schlüssel (public key), sowie ein Zertifikat zur Prüfung der Identität verwendet wird.

Der private Schlüssel, der nur für die Signaturschlüsselinhaberin oder den Signaturschlüsselinhaber (z. B: Signaturkarteninhaberin oder Signaturkarteninhaber) zur Verfügung steht, wird zur Erzeugung einer Signatur verwendet. Der öffentliche Schlüssel dient zur Prüfung von Signaturen und steht allen zur Verfügung. Die Sicherheit der Methode beruht darauf, dass es praktisch unmöglich ist, den privaten Schlüssel aus dem öffentlichen Schlüssel herzuleiten, selbst unter Zuhilfenahme leistungsfähigster Rechnersysteme. Hierbei berechnet sich der öffentliche Schlüssel durch Anwendung einer sogenannten Einwegfunktion aus dem privaten Schlüssel. Daher kann der öffentliche Schlüssel in einem öffentlich zugänglichen Verzeichnis hinterlegt werden, ohne damit den privaten Schlüssel preiszugegeben.

Zertifikate sind elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer Person zugeordnet werden und die Identität dieser Person bestätigt wird. Ein qualifiziertes Zertifikat enthält folgende Angaben:

- den Namen der Signaturschlüsselinhaberin oder des Signaturschlüsselinhabers oder ein der Signaturschlüsselinhaberin oder dem Signaturschlüsselinhaber zugeordnetes unverwechselbares Pseudonym,
- den zugeordneten Signaturprüfschlüssel,
- die Bezeichnung der Algorithmen, mit denen der Signaturprüfschlüssel sowie der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann,
- die laufende Nummer des Zertifikates,
- Beginn und Ende der Gültigkeit des Zertifikates,
- den Namen des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist,
- Angaben über Nutzungseinschränkungen,
- Angaben, dass es sich um ein qualifiziertes Zertifikat handelt,

97 Vgl. § 4 SigV

98 Vgl. § 17 SigV

99 Vgl. auch Grundlagen der elektronischen Signatur, BSI, Bonn 2006, S. 21ff.

- bei Bedarf Attribute der Signaturschlüsselinhaberin oder des Signaturschlüsselinhabers.

Bei der Erzeugung einer elektronischen Signatur an einem elektronischen Dokument wird über eine spezielle Berechnungsfunktion der sogenannte Hashwert berechnet. Dies funktioniert ungefähr so wie bei der Berechnung einer Quersumme aus einer Zahlenkolonne. Dieser Hashwert wird anschließend verschlüsselt. Der so verschlüsselte Wert wird mit dem Dokument und dem Zertifikat zusammengeführt. Dabei entsteht das signierte Dokument. Es besteht allerdings auch die Möglichkeit, den Hashwert (die Signatur) separat zu speichern (abgesetzte Signatur).

Bei der Prüfung einer Signatur wird durch die Prüfsoftware erneut ein Hashwert berechnet. Stimmt der neu berechnete Hashwert mit dem übermittelten Hashwert überein, so ist die Signatur mathematisch gültig und das Dokument wurde nicht verändert. Die folgende Abbildung stellt dieses Prinzip im Überblick dar.

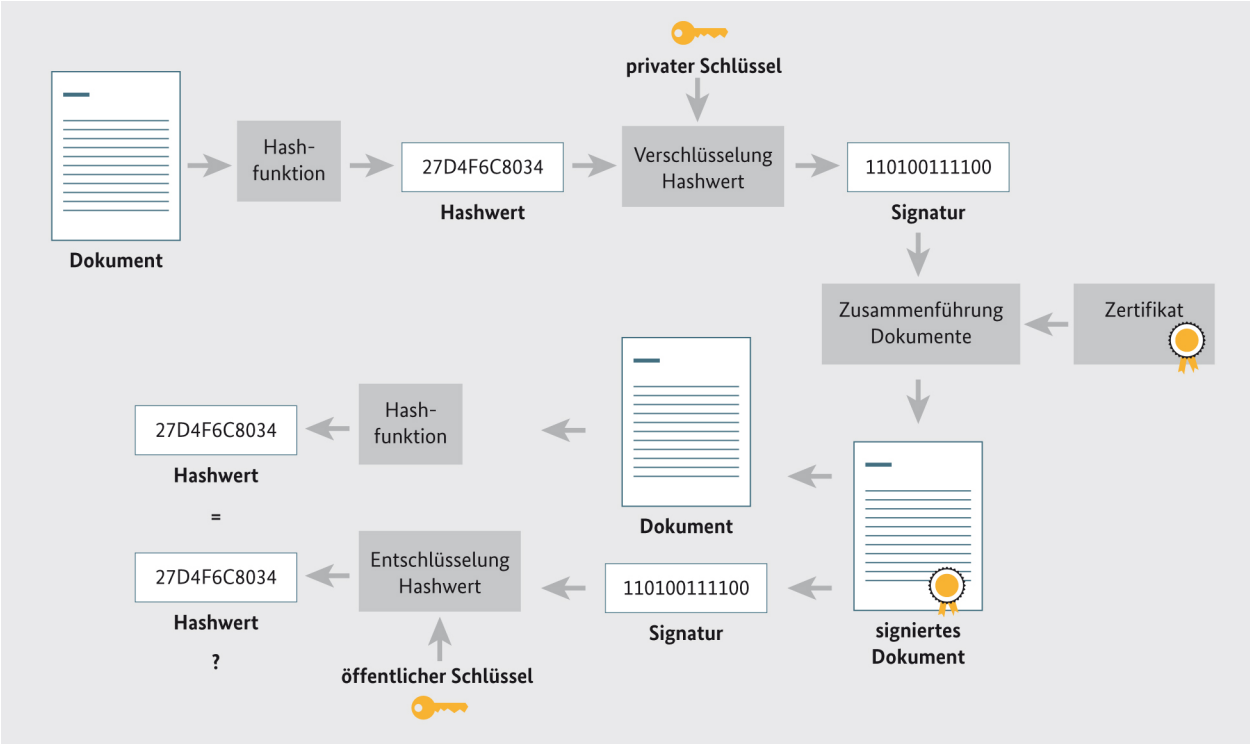


Abbildung 7: Erzeugung und Prüfung einer Signatur[100]

Bei qualifizierten elektronischen Signaturen werden die Schlüssel und die Zertifikate durch einen Zertifizierungsdiensteanbieter, der entweder bei der Bundesnetzagentur akkreditiert ist oder aber den Betrieb angezeigt hat, erzeugt.

Die privaten Schlüssel und Zertifikate werden der Signaturkarteninhaberin bzw. dem Signaturkarteninhaber auf der Signaturkarte zur Verfügung gestellt. Zur Erzeugung einer qualifizierten Signatur an einem Dokument nutzt die Unterzeichnerin oder der Unterzeichner eine sichere Signaturerstellungseinheit und sichere Signaturanwendungskomponenten[101]. Bei der Erzeugung einer Signatur muss die Unterzeichnerin oder der Unterzeichner zur Sicherheit einen PIN-Code eingeben, um ähnlich wie bei einer EC-Karte Missbrauch zu verhindern.

Der Zertifizierungsdiensteanbieter übernimmt die Rolle einer vertrauenswürdigen Stelle (Trust-Center), die bestätigt, dass sie das Zertifikat und die privaten Schlüssel genau einer bestimmten Person (der Unterzeichnerin oder dem Unterzeichner) zur Verfügung gestellt hat. Bei einem positiven Ergebnis einer Signaturprüfung kann man also grundsätzlich davon ausgehen, dass ein elektronisches Dokument auch von der Inhaberin bzw. vom Inhaber des Zertifikates signiert wurde.

100 Vgl. auch BSI, Grundlagen der elektronischen Signatur, Bonn 2006

101 Signaturanwendungskomponenten sind Software- und Hardwareprodukte, die dazu bestimmt sind, Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen, qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen.

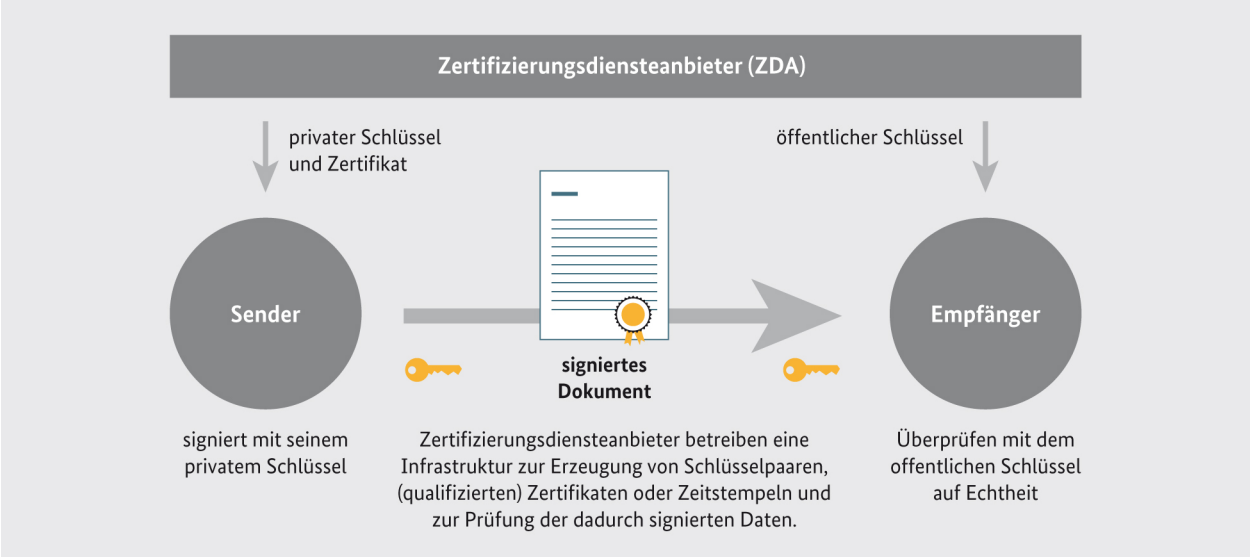


Abbildung 8: Funktion der Zertifizierungsdiensteanbieter[102]

Anbringungsformen

Bei elektronisch signierten Dokumenten ist zu unterscheiden, wie die Signaturen am jeweiligen Dokument angebracht wurden. Folgende Varianten sind möglich:

- Die Signatur wird in das Dokument eingebettet (Signierung des Inhaltes inkl. Metadaten innerhalb des jeweiligen Dokumentes).
- Die Signatur wird in einer separaten Signaturdatei gespeichert (abgesetzte Signatur).
- Die Signatur wird zunächst in einer separaten Signaturdatei gespeichert, im Anschluss aber zusammen mit dem Dokument in einen sogenannten Signaturcontainer zusammengeführt.

Die folgende Abbildung stellt die Möglichkeiten grafisch dar.

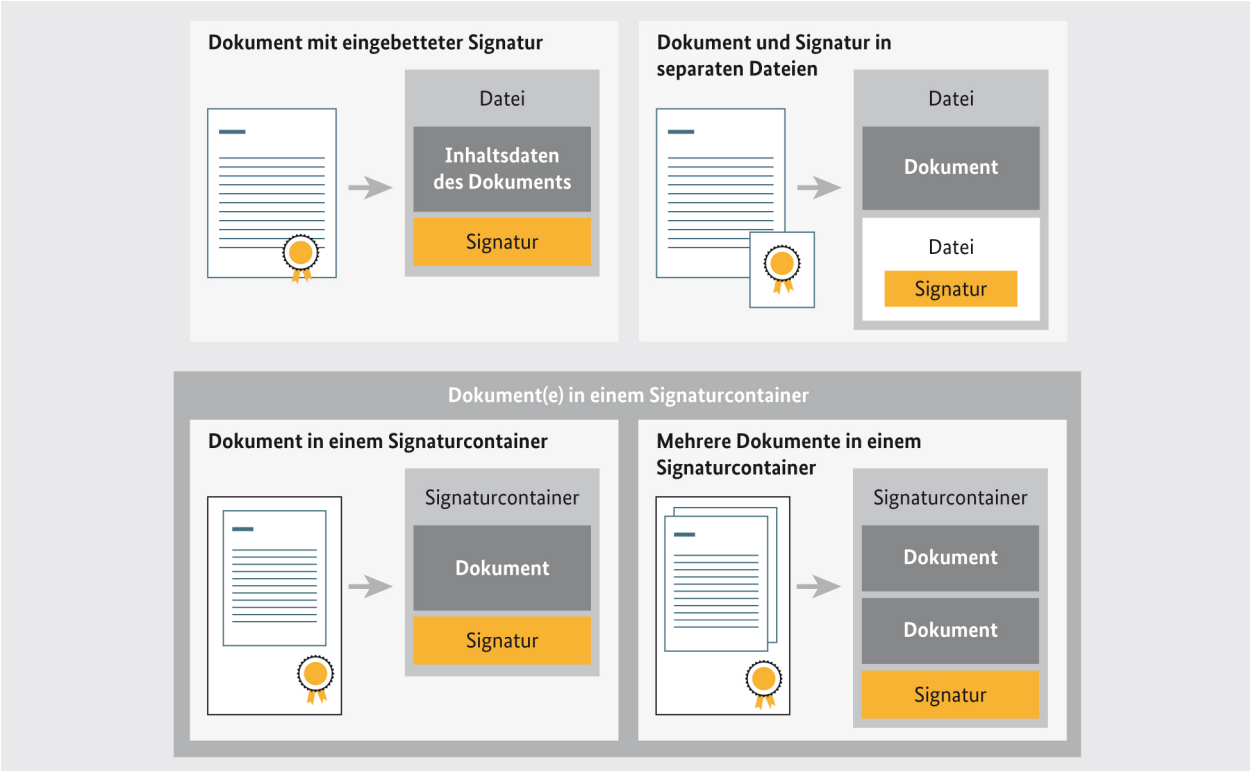


Abbildung 9: Varianten für die Signierung von Dokumenten

102 Vgl. Grundlagen der elektronischen Signatur, BSI, Bonn 2006

Die eingebettete Signatur entspricht in der Dokumentenbehandlung weitgehend dem traditionellen Papiervorgehen, da die Signatur wie eine Unterschrift fest mit dem Dokument verbunden ist. Sie kann z. B. als PDF-Signatur auch in PDF/A-Dateien abgebildet werden, so dass auch die Lesbarkeit der Datei sichergestellt ist. Diese Form der Signatur ist die einfachste Möglichkeit, signierte Dokumente zu verteilen.

Verfügbarkeit und Prüfbarkeit von Zertifikaten

Ein Problem bei der Verwendung qualifizierter Signaturen ist, dass die Berechnungsmethoden für die Erzeugung von Signaturen durch technischen Fortschritt potenziell unsicher werden können. Daher haben Zertifikate eine maximale Gültigkeit von zehn Jahren (§ 14 SigV). In der Regel sind sie zwei bis vier Jahre gültig.

Darüber hinaus müssen die zugrunde liegenden Zertifikate von den Zertifizierungsdiensteanbietern nach Ablauf

der Gültigkeit nur über einen bestimmten Zeitraum gespeichert werden. Diese Speicherung ist nötig, um eine Prüfung der Signatur vornehmen zu können. Bei qualifizierten Zertifikaten beträgt dieser Zeitraum mindestens fünf Jahre, bei qualifizierten Zertifikaten mit Anbieterakkreditierung sind es mindestens 30 Jahre.

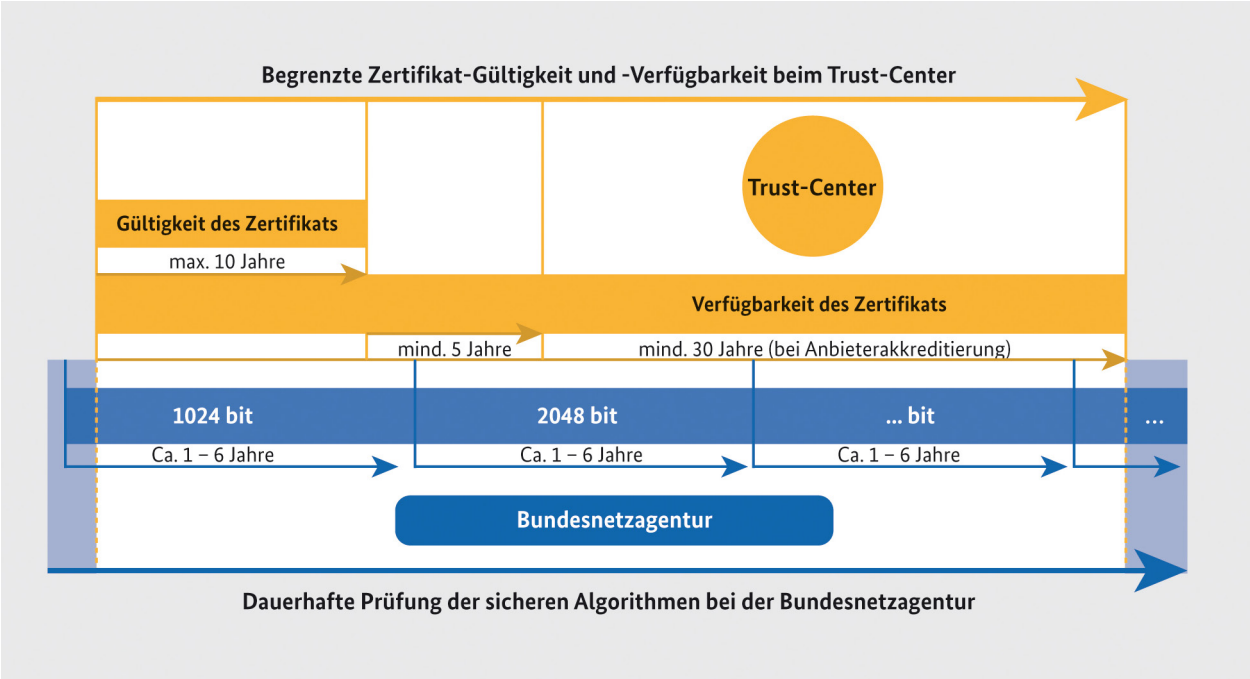


Abbildung 10: Verfügbarkeit und Prüfbarkeit von Zertifikaten

Nach §17 SigV sind signierte Dokumente, die für längere Zeit in signierter Form benötigt werden, durch Anbringen einer neuen Signatur überzusignieren. Die TR-03125 des BSI[103] beschreibt geeignete Maßnahmen. Weitere Ansätze finden sich im Baustein „E-Langzeitspeicherung“ des Organisationskonzeptes elektronische Verwaltungsarbeit.

103 Technische Richtlinie 03125 (TR-03125) des BSI, s. https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html

Literaturverzeichnis

Die Beauftragte der Bundesregierung für Informationstechnik (BfIT), SAGA-Modul Technische Spezifikationen, Version de.bund 5.0.0, 3. November 2011

Die Beauftragte der Bundesregierung für Informationstechnik (BfIT), Grundlagen für den Einsatz von De-Mail in der öffentlichen Verwaltung (V 1.0 vom 21. Juni 2012) des Kompetenzzentrums De-Mail, Quelle: http://www.cio.bund.de/SharedDocs/Publikationen/DE/De-Mail/2012_06_21_cc_de_mail_einsatzszenarien_v1_0_pdf_download.pdf?__blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik (BSI), Grundlagen der elektronischen Signatur, Bonn 2006, Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/esig_pdf.pdf?__blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik (BSI), TR-03107 „elektronische Identitäten und Vertrauensdienste im

eGovernment“, Teile 1 und 2, Quelle: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03107/index_htm.html

Bundesamt für Sicherheit in der Informationstechnik (BSI) IT-Grundschutz-Standards, BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise

Bundesamt für Sicherheit in der Informationstechnik (BSI) IT-Grundschutz-Kataloge, Glossar und Begriffsdefinitionen.

Bundesministerium des Innern (BMI), Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung, http://www.orghandbuch.de/nn_414836/OrganisationsHandbuch/DE/5__Personalbedarfsermittlung/personalbedarfsermittlung-node.html?__nnn=true, Kapitel 5, Stand: Mai 2013

Bundesministerium des Innern, Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Akte, Berlin, Mai 2012

Bundesministerium des Innern, Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Zusammenarbeit, Bundesministerium des Innern, Berlin, Mai 2012

Bundesministerium des Innern, Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Vorgangsbearbeitung, Bundesministerium des Innern, Berlin, Mai 2012

Bundesministerium des Innern, Organisationskonzept elektronische Verwaltungsarbeit – Baustein E-Langzeitspeicherung, Bundesministerium des Innern, Berlin, 2014

Bundesministerium für Wirtschaft und Technologie, Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente, Kapitel 3.2

Impressum

Herausgeber:
Bundesministerium des Innern
Alt-Moabit 101D
10559 Berlin

Dieses Dokument wurde in Zusammenarbeit
mit der Firma IMTB erstellt.

Ansprechpartner:
Bundesministerium des Innern
Referat O1
o1@bmi.bund.de

Berlin, Juli 2014

Gestaltung und Produktion:
MediaCompany – Agentur für Kommunikation GmbH

www.bmi.bund.de

www.bmi.bund.de