Deutscher Bundestag **Drucksache 17/10720**

17. Wahlperiode 13. 09. 2012

Unterrichtung

durch die Bundesregierung

Bericht der Bundesregierung nach Artikel 5 des Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften

Inhaltsverzeichnis

		Seite
A.	**Berichtspflicht**	3
B.	**Umsetzung der Berichtspflicht**	3
C.	**Voraussetzungen für die Ersetzung der Schriftform im öffentlichen Recht**	3
I.	Inhalt und Funktion der Schriftform im Verwaltungsrecht	4
II.	Besonderheiten im Steuerrecht	4
III.	Inhalt und Funktion der Schriftform im Prozessrecht	5
D.	**De-Mail als elektronischer Schriftformersatz alternativ zur qeS**	**5**
I.	Die technische Funktionsweise von De-Mail	5
II.	Die Erfüllung der Schriftformfunktionen durch De-Mail	6
1.	Perpetuierungs-/Abschlussfunktion und Echtheitsfunktion	6
2.	Warnfunktion	7
3.	Identitäts- und Verifikationsfunktion	7
4.	Beweisfunktion	8
5.	Zusammenfassende Bewertung	9
III.	Ersetzung der Schriftform durch De-Mail im Sozial- und Steuerrecht	9
IV.	Ersetzung der Schriftform durch De-Mail im Prozessrecht	9
F.	**Der elektronische Identitätsnachweis nach § 18 Personalausweisgesetz als Schriftformersatz**	9
I.	Die technische Funktionsweise des elektronischen Identitätsnachweises	9

Zugeleitet mit Schreiben des Bundesministeriums des Innern vom 11. September 2012 gemäß Artikel 5 des Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften.

Seite

II. Die Abbildung der Schriftformfunktionen unter Einsatz der Online-Ausweisfunktion 10

1. Einsatz der Online-Ausweisfunktion im Verwaltungsrecht 10

2. Schriftformäquivalenz im Sozial- und Steuerrecht 10

3. Schriftformäquivalenz im Prozessrecht 10

G. Zusammenfassung/Schlussfolgerungen 11

A. Berichtspflicht

Artikel 5 des Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften vom 28. April 2011 (De-Mail-Gesetz, BGBl. 2011, Teil 1, Nr. 19, S. 666 ff.) hat folgenden Wortlaut:

„Die Bundesregierung berichtet dem Deutschen Bundestag innerhalb eines halben Jahres nach Inkrafttreten des De-Mail-Gesetzes darüber, ob und gegebenenfalls in welchen Rechtsgebieten De-Mail oder der elektronische Identitätsnachweis nach § 18 des Personalausweisgesetzes die einzelnen Funktionen der Schriftform alternativ zur qualifizierten elektronischen Signatur ersetzen könnte. Hierfür wird auch das Fachrecht auf Einsatzmöglichkeiten überprüft. Dabei sollten insbesondere Regelungen untersucht werden, die die Kommunikation mit staatlichen Stellen betreffen."

Zur Begründung dieser Berichtspflicht wird in der Gesetzesbegründung ausgeführt:

„Die vorgeschlagene Regelung betrifft eine Berichtspflicht der Bundesregierung, die zum Ziel haben soll, zu ermitteln, ob und gegebenenfalls in welchen Rechtsgebieten De-Mail oder der elektronische Identitätsnachweis die einzelnen Funktionen der Schriftform (Identitätsfunktion, Echtheitsfunktion, Verifikationsfunktion, Beweisfunktion, Perpetuierungsfunktion, Abschlussfunktion und Warnfunktion) alternativ zur qualifizierten Signatur ersetzen könnte. Aufbauend auf dem Ergebnis dieser Untersuchung könnten in einem weiteren Gesetzgebungsverfahren Anpassungen an das geltende Recht vorzunehmen sein. Hierzu bietet sich vor allem das Gesetzgebungsverfahren zu einem E-Government-Gesetz an."

B. Umsetzung der Berichtspflicht

Kern der Berichtspflicht ist die Prüfung, inwieweit De-Mail oder der elektronische Identitätsnachweis nach § 18 des Personalausweisgesetzes geeignet sind, im elektronischen Rechtsverkehr neben der qualifizierten elektronischen Signatur (im Folgenden: qeS) die Schriftform zu ersetzen[1]. Die Online-Ausweisfunktion (auch eID-Funktion genannt) ist Bestandteil des neuen Personalausweises (im Folgenden: nPA).

Da insbesondere Regelungen untersucht werden sollen, die die Kommunikation mit staatlichen Stellen betreffen, wurden schwerpunktmäßig verwaltungsrechtliche Vorschriften geprüft, die in ihrem jeweiligen Anwendungsbereich die Voraussetzungen der Schriftform oder ihre Ersetzung allgemein regeln. Dies sind insbesondere § 3a Verwaltungsverfahrensgesetz (VwVfG), § 87a Abgabenordnung (AO) und 36a Erstes Buch Sozialgesetzbuch (SGB I).

Angesichts der kurzen Berichtsfrist konnte nicht untersucht werden, inwieweit sämtliche im Fachrecht in vierstelliger Zahl enthaltenen Schriftformanordnungen so umgestaltet werden können, dass sie auch durch De-Mail oder den Einsatz des nPA erfüllt werden könnten.

C. Voraussetzungen für die Ersetzung der Schriftform im öffentlichen Recht

Im Prozessrecht und im materiellen öffentlichen Recht existieren keine Vorschriften, die die Anforderungen an die Schriftform für alle Schriftformerfordernisse allgemein festlegen. Soweit nicht eine gesetzliche Bestimmung ausdrücklich eine eigenhändige Unterschrift auf einem Dokument verlangt, muss im Prozessrecht im Wege der Auslegung ermittelt werden, ob dies aus anderen Gründen zwingend ist oder ob eine Entsprechung zur bloßen Textform genügt. Ein Unterschriftserfordernis kann durch Gesetz ausdrücklich angeordnet sein, insbesondere durch den Begriff „handschriftliche Unterzeichnung". Das Unterschriftserfordernis kann sich aber auch aus Umschreibungen oder aus der Natur der Sache ergeben. Aus Begriffen wie „Schriftstück" oder „schriftlich" kann nicht zwingend auf ein Unterschriftserfordernis geschlossen werden.

In allen Bereichen des öffentlichen Rechts finden sich aber Vorschriften, die regeln, wie die Schriftform im elektronischen Rechtsverkehr ersetzt werden kann:

- § 3a VwVfG, § 87a AO und § 36a SGB I schaffen dafür eine besondere elektronische Form;
- in § 130a Zivilprozessordnung (ZPO), § 41a Strafprozessordnung (StPO), § 46b Arbeitsgerichtsgesetz (ArbGG), § 65a Sozialgerichtsgesetz (SGG),
- § 55a Verwaltungsgerichtsordnung (VwGO) und § 52a Finanzgerichtsordnung (FGO) wird bestimmt, wie die prozessuale Schriftform bei elektronischen Erklärungen ersetzt werden kann.

Diese Vorschriften sind zwar im Einzelnen verschieden ausgestaltet. Gemeinsam ist ihnen aber, dass die Schriftform im elektronischen Rechtsverkehr jedenfalls dadurch ersetzt werden kann, dass das elektronische Dokument, welches die formbedürftige Erklärung enthält, mit einer qualifizierten elektronischen Signatur (qeS) versehen wird (zu Ausnahmen im Steuerrecht s. unten II.). Optional können (z. B. im Bereich der StPO, der VwGO, der FGO und des SGG) die Bundesregierung und die Landesregierungen für ihren Bereich durch Rechtsverordnung bestimmen, dass neben der qeS auch ein anderes „sicheres Verfahren" zugelassen wird. Dieses muss die Authentizität und Integrität des übermittelten Dokuments (dauerhaft) sicherstellen, vgl. § 41a StPO, § 55a VwGO, § 65a SGG, § 52a FGO.

Die in diesen Vorschriften vorgesehenen Formanforderungen, insbesondere die qeS, gewährleisten, dass die elektronische Form im Wesentlichen die gleichen Funktionen wie die Schriftform erfüllen kann. De-Mail oder die Online-Ausweisfunktion des nPA können als Alternativen zur qualifizierten elektronischen Signatur in diese

[1] Aufgrund seiner zusätzlichen Sicherheitsfunktionen ist De-Mail für eine Vielzahl von Anwendungsfällen geeignet, bei denen heute ein Papierbrief verwendet wird. Für bestimmte Anwendungsfälle fordert das Gesetz zusätzlich, dass der entsprechende Vorgang handschriftlich unterschrieben wird (Schriftform). Dies betrifft allerdings nur einen Bruchteil aller Kommunikationsvorgänge. Insoweit geht es hier um die Prüfung einer Ausweitung des Anwendungsbereichs von De-Mail.

Vorschriften nur aufgenommen werden, wenn auch eine so ausgestaltete elektronische Form im Wesentlichen die gleichen Funktionen wie die Schriftform erfüllen könnte. Dies wird nachfolgend für die Formvorschriften in § 3a VwVfG, § 87a AO und § 36a SGB I mit Blick auf den Inhalt und die Funktionen der einzelnen Schriftform, die ersetzt werden soll, gesondert dargestellt.

I. Inhalt und Funktion der Schriftform im Verwaltungsrecht

In § 10 VwVfG ist der Grundsatz der Nichtförmlichkeit des Verwaltungsverfahrens verankert. Hiernach können auch rechtsverbindliche Erklärungen formfrei abgegeben werden, soweit nicht besondere Vorschriften eine bestimmte Form verlangen – wie etwa in § 57 VwVfG. Insoweit können die Verfahrensbeteiligten immer auch einfach auf elektronischen Weg kommunizieren, etwa per einfacher E-Mail, wenn nach § 3a Absatz 1 VwVfG ein Zugang eröffnet wurde.

Eine Vorschrift, die – vergleichbar etwa § 126 BGB für das Zivilrecht – allgemein festlegt, wie die Schriftform zu erfüllen ist, fehlt im öffentlichen Recht. Der Inhalt der einzelnen öffentlich-rechtlichen Schriftformerfordernisse ist unterschiedlich, abhängig von ihrem Zweck. Je nach Ausgestaltung sind auch die möglichen Funktionen der Schriftform verschieden ausgeprägt[2]. Insgesamt kann auch die Schriftform im öffentlichen Recht folgende Funktionen haben:

– **Perpetuierungsfunktion**

  Schriftform setzt auch im Verwaltungsrecht immer die Verkörperung der Erklärung in einer Urkunde voraus. Durch die Verkörperung der Erklärung in einer Urkunde (Urkundeneinheit) wird gewährleistet, dass die Erklärung dauerhaft festgehalten ist. Dies ermöglicht es, ihren Inhalt zu überprüfen.

– **Warnfunktion**

  Wenn zur Einhaltung der Schriftform die eigenhändige Unterzeichnung der Erklärung erforderlich ist, wird der Erklärende durch den bewussten Akt des Unterzeichnens auf die erhöhte rechtliche Verbindlichkeit und die persönliche Zurechnung der unterzeichneten Erklärung hingewiesen. Hierdurch soll er vor Übereilung geschützt werden.

– **Abschlussfunktion**

  Durch die eigenhändige Unterschrift wird die Erklärung räumlich abgeschlossen; Bestandteil der Erklärung ist grundsätzlich nur, was vor der Unterschrift steht. Die eigenhändige Unterschrift grenzt bei nicht empfangsbedürftigen Erklärungen auch die verbindliche Erklärung vom Entwurf ab.

– **Identitäts- und Verifikationsfunktion**

  Durch eigenhändige Namensunterschrift ist der Aussteller der Urkunde erkennbar und identifizierbar, da die unverwechselbare Unterschrift eine unzweideutige Verbindung zur Person des Unterzeichners herstellt. Die Identität kann im Streitfall z. B. durch einen Unterschriftenvergleich verifiziert werden.

– **Echtheitsfunktion**

  Die räumliche Verbindung der Unterschrift mit der Urkunde, die die Erklärung enthält, stellt einen Zusammenhang zwischen der Erklärung und Unterschrift her. Hierdurch soll gewährleistet werden, dass die Erklärung inhaltlich vom Unterzeichner herrührt und nicht nachträglich verfälscht werden kann.

– **Beweisfunktion**

  Durch die Verkörperung der Erklärung in einer Urkunde, die vom Aussteller eigenhändig unterschrieben ist, wird ein Beweismittel geschaffen. Mit der Urkunde kann bewiesen werden, welchen Inhalt die Erklärung hat und wer sie abgegeben hat. Dieser Beweis kann aufgrund der Verifikationsfunktion der Unterschrift, insbesondere durch einen Unterschriftenvergleich erbracht werden.

In manchen Fällen wollte der Gesetzgeber mit der Formulierung „schriftlich“ in verwaltungsrechtlichen Regelungen etwa vor allem dem Anliegen gerecht werden, in Abgrenzung zur Mündlichkeit den genauen Inhalt von Erklärungen zu dokumentieren. Die Schriftform dient hier deshalb primär dem aus dem Rechtsstaatsprinzip resultierenden Erfordernis der ordnungsgemäßen Aktenführung. Zur Erfüllung dieses behördlichen Dokumentationsinteresses kommt es vorwiegend auf die Perpetuierungsfunktion der Schriftform an, d. h. auf die Verkörperung der Erklärung in archivierbarer Form. Solche Schriftformerfordernisse verlangen häufig nicht die eigenhändige Unterzeichnung der Erklärung.

Gleichwohl kann nach geltender Rechtslage die Schriftform im Verwaltungsrecht nur durch eine besondere elektronische Form ersetzt werden, deren wesentliche Formvoraussetzung die qeS ist (§ 3a Absatz 2 Satz 2 VwVfG) und die im Wesentlichen die gleichen Funktionen wie alle im öffentlichen Recht vorkommenden Schriftformtypen erfüllt – also auch die Schriftformerfordernisse, die einen eigenhändige Unterzeichnung der Erklärung verlangen. Damit werden im Bereich des Verwaltungsrechts in vielen Fällen für den elektronischen Rechtsverkehrs höhere Formanforderungen gestellt als für den papiergebundenen Rechtsverkehr.

II. Besonderheiten im Steuerrecht

Besonderheiten ergeben sich schließlich im Steuerrecht: § 87a AO wurde als Folge der nur schleppend voran kommenden Automatisierungsbemühungen im Bereich der

[2] So geht das Bundesverwaltungsgericht etwa davon aus, dass bei der Widerspruchseinlegung zur Wahrung der Schriftform zwar grundsätzlich die eigenhändige Unterschrift als Bekenntnis des Verfassers zum Inhalt der Erklärung gehört, die Schriftform aber auch gewahrt sein kann, wenn das Widerspruchsschreiben nicht unterschrieben wurde. In diesem Fall muss sich jedoch schon aus der Erklärung allein ohne die Notwendigkeit einer Beweisaufnahme zweifelsfrei ergeben, dass der Aussteller die Erklärung so in den Rechtsverkehr geben wollte (vgl. BVerwGE 30, S. 274).

rechtsverbindlichen Kommunikation zwischen Steuerpflichtigen und Finanzbehörden bereits frühzeitig um eine Öffnungsklausel in Absatz 6 erweitert. Darauf basierend wurde bereits im Jahr 2003 die „Steuerdaten-Übermittlungsverordnung (StDÜV)“ erlassen, deren Anforderungen an Programme und deren Regelungen zur Authentizität, Vertraulichkeit sowie Integrität der Datenübermittlungen zwischenzeitlich auch im Bereich des Verbrauchsteuerrechts ihre Entsprechung gefunden haben.

Die in § 87a Absatz 6 Satz 1 AO zunächst enthaltene Befristung bis 31. Dezember 2011 ist als Ergebnis des Evaluierungsberichts des Bundesministeriums der Finanzen (BMF) vom Januar 2011 im Zuge des Steuervereinfachungsgesetzes 2011 vom 1. November 2011 (BGBl. I S. 2131) aufgehoben worden. Der Evaluierungsbericht des BMF ist zu dem eindeutigen Ergebnis gekommen, dass das von den Finanzbehörden eingeführte andere sichere Verfahren (ELSTER) Authentizität, Vertraulichkeit und Integrität der Steuerdaten in gleichem Maße sicherstellt wie die qeS. Die dabei genutzten Mechanismen (Algorithmen und Schlüssel) entsprechen technisch und sicherheitstechnisch denen der qeS. Eine Nutzung und Einbindung der qeS im Rahmen des ELSTER- Verfahrens ist dessen ungeachtet jederzeit möglich und erleichtert einzelne Funktionen (ELSTER- Plus).

Zudem wird als Folge des Steuervereinfachungsgesetzes 2011 künftig zur Authentifizierung des Datenübermittlers auch der elektronische Identitätsnachweis des Personalausweises genutzt werden können. Die dazu erforderlichen Daten dürfen zusammen mit den übrigen übermittelten Daten gespeichert und verwendet werden (§ 87a Absatz 2 Satz 2 AO). Die verfahrensrechtlichen Voraussetzungen zur Einbindung des nPA sind durch das BMF gemeinsam mit BMI noch zu bestimmen (§ 150 Absatz 6 Satz 5 AO).

III. Inhalt und Funktion der Schriftform im Prozessrecht

Im Prozessrecht gilt ein spezieller Schriftformbegriff, auf den beispielsweise § 130a ZPO für die Frage, ob ein elektronisches Dokument qualifiziert elektronisch signiert werden soll, Bezug nimmt (vgl. zum Prozessrecht unten D.IV.).

D. De-Mail als elektronischer Schriftformersatz alternativ zur qeS

I. Die technische Funktionsweise von De-Mail

Jeder De-Mail-Nutzer muss sich zur Einrichtung seines De-Mail-Kontos zunächst sicher identifizieren (§ 3 Absatz 2 und 3 De-Mail-Gesetz). Dies kann auf nicht-elektronischem Wege etwa mit dem Post-Ident-Verfahren, bei dem in einer Filiale der Deutschen Post AG oder gegenüber einem Zusteller ein Ausweisdokument vorgelegt wird, oder über andere Verfahren mit vergleichbaren Anforderungen geschehen. Die elektronische Erstidentifizierung kann anhand der Online-Ausweisfunktion oder anhand einer qualifizierten elektronischen Signatur nach § 2 Nummer 3 des Signaturgesetzes erfolgen.

Nachdem der De-Mail-Nutzer sein Konto erhalten hat, kann er sich wahlweise mit normalem Authentisierungsniveau (d. h. z. B. mit Benutzernamen und Passwort, § 4 Absatz 1 Satz 3 De-Mail-Gesetz) oder mit hohem Authentisierungsniveau (§ 4 Absatz 1 Satz 2 und Absatz 2 De-Mail-Gesetz, d. h. mit „Besitz und Wissen“ unter Nutzung z. B. des nPA, mobiler TAN-Verfahren oder anderer Verfahren) an seinem Konto anmelden. Wenn der Nutzer von seinem De-Mail-Konto eine De-Mail versendet, wird diese über einen verschlüsselten Kanal zu dessen De-Mail-Provider geleitet, über den die Daten – analog etwa der Nutzung von Online-Banking-Diensten – verschlüsselt übermittelt werden. Bei dem Provider des Absenders werden die Daten automatisiert entschlüsselt, auf Schadsoftware überprüft und anschließend für den Versand an den Provider des Empfängers erneut verschlüsselt. Nach Eingang beim Provider des Empfängers wird die Nachricht wiederum automatisiert entschlüsselt und auf Schadsoftware überprüft. Schließlich ruft sie der Empfänger über einen verschlüsselten Kanal ab.

Neben diesem Standardverfahren kann der Versender zusätzlich eine oder mehrere der folgenden Versandoptionen wählen:

– Der Versender kann sich den Versand der Nachricht bestätigen lassen (§ 5 Absatz 7 De-Mail-Gesetz). In diesem Fall erhält er eine vom Provider des Versenders qualifiziert elektronisch signierte Bestätigung, dass er diese Nachricht verschickt hat. Die Signatur dieser Bestätigung des De-Mail-Providers über den Versand der Nachricht umfasst alle Inhalte und alle zu diesem Zeitpunkt vorliegenden Metadaten (Versandzeitpunkt, Authentisierungsniveau etc.) der entsprechenden De-Mail.

– Der Versender kann sich den Eingang der Nachricht beim Empfänger bestätigen lassen (§ 5 Absatz 8 De-Mail-Gesetz). In diesem Fall erhalten Versender und Empfänger eine vom Provider des Empfängers qualifiziert elektronisch signierte Bestätigung, dass diese Nachricht im Postfach des Empfängers eingegangen ist. Die Signatur dieser Bestätigung des De-Mail-Providers über den Eingang der Nachricht umfasst alle Inhalte und zu diesem Zeitpunkt vorliegenden Metadaten der entsprechenden De-Mail.

– Der Versender einer Nachricht kann von seinem Provider bestätigen lassen, dass er zum Zeitpunkt des Versands dieser De-Mail mit hohem Authentisierungsniveau i. S. v. § 4 De-Mail-Gesetz angemeldet war (§ 5 Absatz 5 De-Mail-Gesetz). Dies bedeutet, dass sich der Versender zum Schutz gegen eine unberechtigte Anmeldung unter Einsatz von zwei, voneinander unabhängigen Sicherungsmitteln an seinem De-Mail-Konto anzumelden hat. In diesem Fall wird die entsprechende De-Mail vom Provider des Versenders bei der Absendung vom De-Mail-Konto qualifiziert elektronisch signiert. Die Signatur dieser Bestätigung des De-Mail-Providers über den Versand der Nachricht

mit hohem Authentisierungsniveau umfasst alle Inhalte und zu diesem Zeitpunkt vorliegenden Metadaten der entsprechenden De-Mail. Diese Versandoption wird auch als „absenderbestätigt“ bezeichnet[3].

– Eine öffentliche Stelle, die zur förmlichen Zustellung nach den Vorschriften der Prozessordnungen und der Gesetze, die die Verwaltungszustellung regeln, berechtigt ist, kann eine Abholbestätigung verlangen (§ 5 Absatz 9 De-Mail-Gesetz). Aus der Abholbestätigung ergibt sich, dass sich der Empfänger nach dem Eingang der Nachricht im Postfach an seinem De-Mail-Konto sicher im Sinne des § 4 angemeldet hat und auf diese Nachricht zugreifen konnte.

– Der Versender kann bestimmen, dass eine sichere Anmeldung mit hohem Authentisierungsniveau i. S. v. § 4 De-Mail-Gesetz für das Abholen der Nachricht erforderlich ist (§ 5 Absatz 4 De-Mail-Gesetz). Dies bedeutet, dass sich der Empfänger zum Schutz gegen eine unberechtigte Anmeldung unter Einsatz von zwei, voneinander unabhängigen Sicherungsmitteln an seinem De-Mail-Konto anzumelden hat. Meldet sich der Empfänger nur mit normalem Authentisierungsniveau an (Benutzername und Passwort), kann er auf die entsprechende De-Mail nicht zugreifen.

Zusätzlich zu den Sicherheitsfunktionen bzw. Versandoptionen von De-Mail kann der Nutzer, sofern er entsprechende Technologien auf seinem Endgerät installiert hat, die mit De-Mail übermittelten Inhalte auch Ende-zu-Ende verschlüsseln. Solche zusätzlich Ende-zu-Ende-verschlüsselten Inhalte können dann nur durch den jeweiligen Empfänger (und nicht durch den De-Mail-Provider) entschlüsselt werden.

Aufgrund seiner gegenüber der einfachen E-Mail bestehenden zusätzlichen Sicherheitsfunktionen, die durch das De-Mail-Gesetz sowie die der Akkreditierung zu Grunde liegenden Technischen Richtlinien De-Mail für alle De-Mail-Provider verbindlich vorgegeben werden, ist De-Mail für eine Vielzahl von Anwendungsfällen der elektronischen Kommunikation geeignet, bei denen heute ein Papierbrief verwendet wird.

Das gilt vor allem bei der Nutzung der Versandoption „absenderbestätigt“. Auf Grund dieser Versendungsform kann der De-Mail-Nutzer auf Empfängerseite davon ausgehen, dass die De-Mail tatsächlich von derjenigen natürlichen Person stammt, die Inhaberin des jeweiligen De-Mail-Kontos ist (sichere Anmeldung), und feststellen, ob die De-Mail nach der Versendung verändert wurde (qeS des Providers). Auf diese Weise kann er den per De-Mail versandten Erklärungsinhalt dem Erklärenden zuordnen. Die Signatur des Providers erfasst alle Inhalte der De-Mail und auch die dazugehörigen Metadaten. Anders als bei der Ersetzung der Schriftform durch Verwendung der qeS wird jedoch nicht das einzelne elektronische Dokument, vom Erklärenden selbst signiert, sondern die gesamte De-Mail einschließlich beigefügter Anlagen vom De-Mail-Provider. Das bedeutet, dass immer die gesamte De-Mail (Nachricht mit sämtlichen Anlagen) gespeichert oder weitergeleitet werden muss, wenn die Signaturfunktion erhalten bleiben soll.

Werden per De-Mail Dokumente versandt, die selbst mit einer qeS versehen sind, kann mit diesen dagegen auch außerhalb der De-Mail-Nachricht wie mit einem qualifiziert signierten Dokument umgegangen werden.

II. Die Erfüllung der Schriftformfunktionen durch De-Mail

Soweit eine generelle Regelung zur elektronischen Erfüllung der Schriftform durch De-Mail in § 3a Absatz 2 VwVfG erfolgen soll, muss De-Mail in der Lage sein, sämtliche unter I. genannten Funktionen der Schriftform für die Zwecke des Verwaltungsrechts ausreichend zu erfüllen.

1. Perpetuierungs-/Abschlussfunktion und Echtheitsfunktion

Bei der Verkörperung der Erklärung in einer Urkunde wird gewährleistet, dass die Erklärung dauerhaft festgehalten und ihr Inhalt überprüft werden kann (Perpetuierungsfunktion). Durch die eigenhändige Unterzeichnung der Urkunde wird die Erklärung räumlich abgeschlossen. Die Abschlussfunktion der Unterschrift schafft Klarheit über den Inhalt der Erklärung. Nur was vor der Unterschrift steht, ist formgültig erklärt. Die Verbindung von Erklärung und Unterschrift soll auch die Echtheit gewährleisten. Sie soll verhindern, dass der Inhalt der Urkunde unbemerkt verändert, insbesondere ergänzt werden kann.

Eine Erklärung die in einer De-Mail enthalten ist, bleibt wie eine Erklärung, die in einer Urkunde verkörpert ist, für eine ausreichende Dauer lesbar und überprüfbar, wenn die De-Mail auf einem Datenträger gespeichert wird. Sie kann beliebig aufgerufen, am Bildschirm gelesen oder ausgedruckt werden. Die Perpetuierungsfunktion wird damit erfüllt.

Grundsätzlich kann eine „absenderbestätigte“ De-Mail, deren Versand mit hohem Authentisierungsniveau vom Provider mit einer qeS bestätigt wird, auch eine vergleichbare Abschluss- und Echtheitsfunktion wie eine eigenhändig unterzeichnete Urkunde haben. Wenn der Erklärende die De-Mail absendet, erstellt der De-Mail-Provider einen sogenannten Hashwert (eine Art Prüfsumme) zu dieser De-Mail und versieht diesen Hashwert mit einer qeS. Dieser signierte Hashwert ist Bestandteil der übermittelten De-Mail, die sich nach Abschluss des Kommunikationsvorgangs im Verfügungsbereich sowohl des Absenders („gesendete De-Mails“) als auch des Empfängers („De-Mail-Posteingang“) befindet. Diese De-Mail kann als digitale Datei abgespeichert und dann auf einem Datenträger oder als Anhang einer De-Mail oder auch einer einfachen E-Mail an Dritte weitergeleitet werden. Jeder Empfänger der so weitergeleiteten De-Mail kann seinerseits überprüfen und nachweisen, dass der gesamte Inhalt der Nachricht (Betreff, Nachrichtentext, Anhänge) nicht verändert wurde. Hierfür wird mittels einer geeigneten Software, die bei-

[3] Vgl. Technischen Richtlinie 01201 De-Mail, auf die in § 18 Absatz 2 des De-Mail-Gesetzes Bezug genommen wird).

spielsweise über die De-Mail-Provider zum Download angeboten werden kann, der Hashwert der betreffenden De-Mail erneut erzeugt und mit dem durch den Provider signierten Hashwert verglichen. Sind beide Werte identisch, handelt es sich um die unveränderte De-Mail des Erklärenden. Wurde hingegen auch nur ein Buchstabe des Betreffs, des Nachrichtentextes oder einer der übermittelten Anlagen verändert, stimmen die Hashwerte nicht mehr überein. Bei dem beschriebenen Prüfungsverfahren kommt die Technik des Signaturverfahrens zur Anwendung, die ihre Grundlage im Signaturgesetz hat. Die Anbringung der Signatur durch den De-Mail-Provider erfolgt nach den Vorgaben des Signaturgesetzes sowie der Bundesnetzagentur.

Gegenüber einem handschriftlich unterschriebenen Dokument und einem vom Erklärenden selbst qualifiziert signierten elektronischen Dokument besteht bei einer De-Mail die Besonderheit, dass sich die zur Bestätigung des Versandes vom De-Mail-Provider aufgebrachte Signatur stets auf die gesamte De-Mail bezieht, das heißt neben Betreff und Nachrichtentext auch die ggf. der De-Mail beigefügten Anhänge erfasst. Anders als etwa beim Versand eines handschriftlich unterschriebenen Vertrages nebst weiteren unverbindlichen Entwürfen in einem Briefumschlag können mit De-Mail somit nicht einzelne Inhalte einer Nachricht signiert werden. Die Abschlussfunktion bezieht sich mithin stets auf den gesamten Inhalt der De-Mail, nicht lediglich auf einzelne Dokumente.

Demgegenüber besteht bei der eigenhändigen Signierung eines elektronischen Dokuments mit qeS eine größere Nähe zur Unterzeichnung eines schriftlichen Dokuments. Allerdings kann sich auch die qeS und das mit ihr signierte Dokument, wenn es sich etwa um ein Word-Format handelt, in zwei getrennten Dateien befinden, die bei elektronischer Versendung vom Empfänger ebenfalls gemeinsam abgespeichert werden müssen. Zudem können auch ganze Dokumentenarchive (z. B. als .zip-Dateien) mit einer einzigen qeS signiert werden. Es liegt deshalb bei De-Mail wie qeS letztlich gleichermaßen in der Hand des Nutzers, die Technik sachgerecht einzusetzen und bei der elektronischen Abgabe von Erklärungen, für die Schriftform vorgesehen ist, von der Bildung unzusammenhängender Konvolute abzusehen. Im Verwaltungsrecht kann dem auch dadurch entgegengewirkt werden, dass die Verwaltung die Verfahrensbeteiligten durch entsprechende Hinweise oder Vorgaben davon abhält. Soweit eine staatliche Stelle ihrerseits formbedürftige Dokumente per De-Mail versendet, kann ein sachgerechter Gebrauch ohnehin unterstellt werden.

2. Warnfunktion

Durch das Erfordernis der eigenhändigen Namensunterschrift wird den Erklärenden deutlich vor Augen geführt, dass sie rechtserhebliche Erklärungen abgeben. Es ist tief im Bewusstsein der Teilnehmer am Rechtsverkehr verankert, dass die eigenhändige Unterschrift eine rechtliche Bindung begründet.

Bei De-Mail wird dem Nutzer über verschiedene Mechanismen zwar direkt und indirekt verdeutlicht, dass die Verwendung dieser Technik einen höheren Grad der Verbindlichkeit hat als beispielsweise eine einfache E-Mail. So erhalten natürliche Personen nur dann ein De-Mail-Konto, wenn sie sich vorher unter Vorlage eines Personaldokuments persönlich identifiziert haben. Ferner müssen die künftigen De-Mail-Provider umfassende Informationspflichten gegenüber den Inhabern von De-Mail-Konten erfüllen, insbesondere im Rahmen der Erstidentifizierung. Sie müssen über sämtliche Funktionen von De-Mail und deren Wirkungsweise aufklären. Ferner muss sich der Nutzer, um eine absenderbestätigte De-Mail versenden zu können, für diese De-Mail-Sitzung mit hohem Authentisierungsniveau (also z. B. mit dem neuen Personalausweis) an dem De-Mail-Konto anmelden und aktiv die Versandoption „absenderbestätigt“ für die zu versendende De-Mail auswählen, über deren Wirkungsweise bei Eröffnung des De-Mail-Kontos aufgeklärt wurde.

Es kann jedoch nicht ohne weiteres davon ausgegangen werden, dass die Nutzung eines De-Mail-Kontos dem Erklärenden in gleicher Weise wie die eigenhändige Unterschrift vor Augen führt, dass er eine rechtliche Bindung begründet. Insbesondere die Erstidentifizierung und die Information über die einzelnen Versandoptionen stehen nicht in so engem Zusammenhang zur jeweiligen Erklärung wie die eigenhändige Unterschrift. Auch die Wahl der Versandoption „absenderbestätigt“ dient primär der besseren Dokumentation von Abgabe und Zugang der jeweiligen Erklärung, die einen beliebigen Inhalt haben kann und nicht immer rechtsgeschäftlicher Natur sein muss.

Eine Gleichstellung könnte allerdings durch Änderung des De-Mail-Gesetzes erreicht werden, um eine zusätzliche Funktion zum „Einschalten“ der elektronischen Form, etwa in Form des Anklickens einer besonders bezeichneten Schaltfläche (z. B. „elektronische Form“), festzulegen. Damit würde den Nutzern nachhaltig verdeutlicht, dass sie rechtsverbindliche Erklärungen in elektronischer Form abgegeben, indem sie die Funktion „absenderbestätigt“ über den besonderen Formbutton nutzen. Dass diese Schaltfläche betätigt wurde, wäre auch für den Empfänger der Erklärung erkennbar und nachweisbar zu machen.

3. Identitäts- und Verifikationsfunktion

Bei der Schriftform ist der Erklärende durch die eigenhändige Namensunterschrift auf der Urkunde erkennbar und identifizierbar. Die unverwechselbare Unterschrift schafft die Verbindung zur Person des Erklärenden. Seine Identität kann im Streitfall z. B. anhand der Urkunde durch einen Unterschriftenvergleich verifiziert werden.

Bei einer De-Mail, die eine natürliche Person abgibt, die mit hohem Authentifizierungsniveau bei seinem De-Mail-Konto angemeldet ist, ist die erklärende Person aufgrund der Erstidentifikation und der sicheren Anmeldung identifizierbar. Durch die qeS des Providers wird die sichere Anmeldung dokumentiert und überprüfbar, d. h. sie ist auch verifizierbar. Die Identifikations- und Verifikationsfunktion sind bei De-Mail daher gegeben, wenn der Erklärende die De-Mail von einem De-Mail-Konto versendet, das für eine natürliche Person eingerichtet wurde (vgl. dazu auch unten 4.).

Soweit eine Behörde De-Mail nutzt, um schriftformbedürftige Erklärungen zu versenden, erscheint die Zurechenbarkeit zu dieser Stelle hingegen ausreichend, wenn nicht unmittelbar feststellbar sein muss, wer für die Behörde gehandelt hat. Die gemäß Artikel 20 Absatz 3 des Grundgesetzes an Gesetz und Recht gebundene Exekutive kann ggf. durch die Ausgestaltung der Verbindung zwischen Arbeitsplatzrechner und Gateway oder sonstige interne Maßnahmen im Rahmen der Vorgangsbearbeitung und Aktenführung sicherstellen, dass eine sichere Identifikation der natürlichen Person möglich ist, die die Erklärung für die Behörde abgegeben hat.

Eine vergleichbare Konstellation liegt auch bei der Nutzung von De-Mail durch Rechtsanwalts- oder Steuerberaterkanzleien vor. Auch hier kann aufgrund organisatorischer Maßnahmen innerhalb der Kanzlei die Zurechnung eines Schriftsatzes zu dem jeweiligen Berufsträger in ausreichendem Maße gewährleistet werden. Wenn der Rechtsanwalt künftig per De-Mail mit Gerichten kommuniziert, sollen die Prozessordnungen vorsehen, dass die anwaltlichen Schriftsätze die Wiedergabe der Unterschrift des Anwalts enthalten. Eine vergleichbare Regelung besteht bereits jetzt für die anwaltliche Kommunikation mit den Gerichten per Telefax (§ 130 Nummer 6 ZPO).

Für den Bereich der Justiz ist jedoch unverzichtbar, dass z. B. eine gerichtliche Entscheidung unmittelbar den oder die Entscheidenden erkennen lässt. Entsprechend schreibt § 130b ZPO vor, dass am Ende eines gerichtlichen elektronischen Dokuments der Name der verantwortenden Person hinzugefügt und das Dokument mit einer qeS versehen wird. Die Versendung dieses signierten Dokumentes über De-Mail ist bereits jetzt möglich (s. u. IV.).

4. Beweisfunktion

Die Einhaltung der Schriftform im Verwaltungsrecht durch Bürger bzw. Unternehmen schafft, wenn ihre Erfüllung nicht nur die Verkörperung in einer Urkunde vorsieht, sondern auch verlangt, dass die Urkunde vom Aussteller eigenhändig unterzeichnet wird, ein Beweismittel, nämlich die Privaturkunde. An die eigenhändig unterschriebene Privaturkunde werden die in der Beweisregel des § 416 ZPO vorgesehenen Beweiswirkungen geknüpft. Nach § 416 ZPO begründen Privaturkunden, sofern sie von den Ausstellern unterschrieben sind, den vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen von den Ausstellern abgegeben sind. Ist Aussteller eine Behörde liegt eine öffentliche Urkunde vor, die gemäß § 417 ZPO den vollen Beweis ihres Inhalts begründet. Ihre Echtheit wird gemäß § 437 ZPO bis zum Beweis des Gegenteils vermutet.

Diese Beweiswirkungen können einer in Schriftform abgegeben Erklärung nur beigelegt werden, wenn die Erklärung durch die eigenhändige Unterschrift einer bestimmten Person zugeordnet werden kann. Das ist immer eine natürliche Person. Juristische Personen oder rechtsfähige Personenvereinigungen können, da sie nicht handlungsfähig sind, diese Voraussetzung selbst nicht erfüllen. Eine schriftliche Erklärung, die eine natürliche Person formwirksam abgegeben hat, kann einer juristischen Person oder Personenvereinigung zwar zugerechnet werden, wenn der Erklärende als Vertreter handelt oder die Voraussetzungen für eine Duldungs- oder Anscheinsvollmacht vorliegen. Die Urkunde selbst wird ihnen aber nicht zugerechnet; sie bleibt immer eine Urkunde, die der Erklärende ausgestellt hat. Um festzustellen, ob eine schriftliche Erklärung, die in einer Urkunde enthalten ist, einer anderen Person als dem Aussteller zugerechnet werden kann, muss feststehen, wer der Aussteller ist und unter welchen Voraussetzungen er gehandelt hat.

Dasselbe gilt nach § 371a Absatz 1 ZPO für private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind. Ein Signaturschlüssel, mit dem eine qualifizierte elektronische Signatur erstellt werden kann, ist immer einer bestimmten natürlichen Person zugeordnet, so dass davon ausgegangen werden kann, dass eine Signatur, die nur mit einem bestimmten Signaturschlüssel erstellt werden kann, von dem Signaturschlüsselinhaber erstellt wurde. § 371a Absatz 2 Satz 2 ZPO erklärt im Fall der qualifiziert elektronisch signierten öffentlichen Urkunde die Echtheitsvermutung des § 437 ZPO für entsprechend anwendbar.

Bei Konten für Unternehmen und Behörden sieht De-Mail vor, dass nicht die einzelnen Mitarbeiter dieser Organisationen einzeln identifiziert werden, sondern die entsprechende Organisation. Diese Organisation ist über ein sogenanntes „Gateway“ mit ihrem De-Mail-Provider sicher verbunden. Einzelne Mitarbeitern des Unternehmens oder der Behörde können über dieses Gateway von ihren Arbeitsplätzen aus Versendung von De-Mails veranlassen. Die Art und Weise, wie die Verbindung zwischen den Arbeitsplatzrechnern der Mitarbeiter und dem Gateway ausgestaltet ist, liegt in der Verantwortung der jeweiligen Einrichtung. De-Mail reguliert diese Umsetzung bewusst nicht, weil auf diese Weise eine einfache und kostengünstige Einbindung in die vorhandene E-Mail-Infrastruktur möglich ist.

Aus diesem Grund kann für Unternehmen nicht davon ausgegangen werden, dass die Umsetzung dieser Verbindung innerhalb der Einrichtung so ausgestaltet ist, dass eine beweissichere Zuordnung der jeweiligen Erklärung zum einzelnen Mitarbeiter gewährleistet ist, der von seinem Arbeitsplatz aus eine De-Mail versendet. Das Problem kann gelöst werden, indem diejenigen Mitarbeiter von privaten Einrichtungen, die schriftformwahrende elektronische Erklärungen abgeben sollen, dies von einem De-Mail-Konto tun, für das sie persönlich identifiziert wurden und bei denen eine direkte Verbindung zwischen dem Endgerät des Nutzers und dem De-Mail-Provider sichergestellt ist (sog. „Individual-Konto“).

Unternehmen sollten allerdings nicht gehindert sein, Erklärungen, die in Schriftform abgegeben werden, aber nicht in Schriftform zugehen müssen, über das De-Mail-Konto des Unternehmens zu versenden. Entsprechend können z. B. auch Abschriften von Schriftsätzen, die ein Rechtsanwalt eigenhändig unterzeichnet hat, von einem De-Mail-Konto der Kanzlei von Mitarbeitern der Kanzlei an die Gerichte versendet werden, wenn die Abschrift des

Schriftsatzes den Rechtsanwalt als Urheber erkennen lässt.

Um für eine De-Mail, die von einem De-Mail-Konto einer natürlichen Person versendet wurde, die gleichen Beweiswirkungen zu schaffen, wie für ein qualifiziert elektronisch signiertes Dokument, müsste § 371a ZPO entsprechend erweitert werden. Allerdings könnte immer nur der gesamten De-Mail diese Beweiswirkung beigelegt werden, nicht auch den einzelnen darin enthaltenen Dokumenten. Denn nur anhand der gesamten De-Mail und der ihr beigefügten Metadaten kann der Erklärende identifiziert und festgestellt werden, dass die Erklärung authentisch ist. Sowohl die Verwaltung als auch der Bürger muss als Beweismittel die gesamte De-Mail nebst Metadaten speichern. Werden nur einzelne rechtserhebliche Erklärungen gespeichert, die durch eine De-Mail übermittelt wurden, aber die De-Mail im Übrigen gelöscht, geht das Beweismittel verloren. Von der Verwaltung kann aber erwartetet werden, dass sie mit einer De-Mail so umgeht, dass es nicht zu einem Beweismittelverlust kommt. Bei Bürgerinnen und Bürgern kann durch entsprechende Hinweise der Verwaltung darauf hingewirkt werden, dass sie eine De-Mail so speichern, dass ein Beweismittelverlust vermieden wird.

5. Zusammenfassende Bewertung

Eine absenderbestätigte De-Mail wäre in der jetzigen Ausgestaltung durch das De-Mail-Gesetz zur Ersetzung der Schriftform im Verwaltungsrecht dann geeignet, wenn

- sie von einem Individual-Konto verschickt wird, für das der Absender persönlich identifiziert wurde und bei dem eine direkte Verbindung zwischen dem Endgerät des Nutzers und dem De-Mail-Provider sichergestellt ist oder wenn der Absender eine Behörde ist und nicht unmittelbar feststellbar sein muss, wer für die Behörde gehandelt hat, sowie
- die ausreichende Warnfunktion einer absenderbestätigten De-Mail durch die Einführung einer gesonderten Schaltfläche gewährleistet wird, die zur Abgabe von Erklärungen in elektronischer Form betätigt werden muss.

Um eine Erklärung, die durch eine „absenderbestätigt“ versandte De-Mail abgegeben wurde, einer in Schriftform abgegebenen Erklärung rechtlich vollständig gleichzustellen, müssten ergänzend entsprechende Beweisregelungen getroffen werden.

III. Ersetzung der Schriftform durch De-Mail im Sozial- und Steuerrecht

Für die Ersetzung der Schriftform im Bereich des Sozialrechts (SGB I) und des Steuerrechts (AO) gilt das zum allgemeinen Verwaltungsrecht Ausgeführte entsprechend, wobei für das Steuerrecht die Ausführungen unter C. II. zu berücksichtigen sind. Um die nötige Rechtssicherheit für den Einsatz von De-Mail im Bereich des Steuerrechts zu gewährleisten, ist im Fachgesetz (AO) darüber hinaus klarstellend zu ergänzen, dass die kurzzeitige automatisierte Entschlüsselung der De-Mail-Nachricht durch den Diensteanbieter nicht als „unbefugtes Offenbaren“ im Sinne des § 30 Absatz 2 AO anzusehen ist und keinen Verstoß gegen das Verschlüsselungsgebot nach § 87a Absatz 1 Satz 3 AO darstellt. Entsprechendes gilt für den Bereich des Sozialgeheimnisses hinsichtlich der Vereinbarkeit mit den Maßgaben der §§ 67 ff. SGB X; insoweit ist im SGB X eine Klarstellung vorzunehmen. Ergänzende Empfehlungen der Beauftragten für den Datenschutz des Bundes und der Länder für den Versand von Steuer- und Sozialdaten mittels De-Mail sind zu beachten.

IV. Ersetzung der Schriftform durch De-Mail im Prozessrecht

Für die Übermittlung und die Zustellung gerichtlicher Dokumente steht De-Mail schon jetzt partiell zur Verfügung. Gemäß § 174 Absatz 3 Satz 4 ZPO (darauf verweisen z. B. auch § 56 Absatz 2 VwGO, § 53 Absatz 2 FGO, § 63 Absatz 2 SGG) können elektronische Dokumente an Rechtsanwälte u. a. zuverlässige Personen auch per De-Mail zugestellt werden. Wird ein elektronisches Dokument über De-Mail zugestellt, ist daran zu denken, das Empfangsbekenntnis des § 174 Absatz 4 ZPO durch die Abholbestätigung nach § 5 Absatz 9 De-Mail-Gesetz oder die Eingangsbestätigung nach § 5 Absatz 8 De-Mail-Gesetz zu ersetzen.

Darüber hinaus wird im Einzelnen zu prüfen sein, ob und für welche Verfahrenshandlungen das Sicherheits- und Authentifizierungsniveau der bestehenden De-Mail-Versandoptionen ausreicht, um an die Stelle des unterschriebenen Schriftsatzes (z. B. § 129 ZPO) oder des mit der qeS versehenen Dokumentes (z. B. § 130a Absatz 2 ZPO) zu treten.

F. Der elektronische Identitätsnachweis nach § 18 Personalausweisgesetz als Schriftformersatz

I. Die technische Funktionsweise des elektronischen Identitätsnachweises

Mit dem elektronischen Identitätsnachweis steht den Bürgerinnen und Bürgern eine neue und sichere Möglichkeit zur Identifizierung im Internet zur Verfügung. Dabei handelt es sich um eine sog. Zwei-Faktor-Authentisierung mit Besitz (Ausweis) und Wissen (eID-PIN). Es findet immer eine gegenseitige Authentisierung statt, d. h. nicht nur der Ausweisinhaber authentisiert sich gegenüber einem Onlinedienst, sondern auch der jeweilige Dienst muss sich gegenüber dem Bürger authentisieren. Zur Nutzung der Online-Ausweisfunktion benötigt der Bürger eine spezielle Software sowie ein Kartenlesegerät. Die Bundesregierung stellt eine solche Software kostenfrei zur Verfügung (sog. „AusweisApp“). Es existieren weitere, zum Teil ebenfalls kostenfreie Angebote am Markt.

Technisch und organisatorisch ist der neue Personalausweis in ein eID-Management System eingebettet. Hat sich ein Bürger beispielsweise in einem Online-Shop ein Produkt zum Kauf ausgesucht, wird er in der Regel vom

Dienstanbieter aufgefordert, seinen Namen, Vornamen und Anschrift mitzuteilen, damit die Ware zugestellt werden kann. Dies kann mit der Online-Ausweisfunktion für beide Seiten sicher gewährleistet werden.

Hierzu muss der Bürger zunächst die sog. AusweisApp oder eine vergleichbare Software auf seinem PC installiert haben, sofern die Funktion nicht bereits über sogenannte Plug-Ins, z. B. über den Web-Browser, bereit steht. Diese Software stellt eine verschlüsselte Verbindung zwischen dem Lesegerät und dem Ausweis her und ermöglicht gleichzeitig einen verschlüsselten und damit sicheren Austausch der erforderliche Daten aus dem Chip des Ausweises unmittelbar an den Kommunikationspartner im Internet. Zu Beginn eines solchen Vorgangs wird dem Bürger das Berechtigungszertifikat des Anbieters angezeigt, das vor der Datenübermittlung vom Chip des Ausweises überprüft wird. Ein solches Zertifikat erhalten Diensteanbieter nur nach Prüfung der Vergabestelle für Berechtigungszertifikate des Bundesverwaltungsamts (BVA). Diese prüft, ob der Anbieter die Daten für seinen Geschäftszweck überhaupt benötigt. Selbstverständlich wird hierbei auch die Identität des Anbieters zweifelsfrei festgestellt. Die Zertifikate werden gegen Vorlage des positiven Bescheides des BVA durch Trust Center am Markt ausgestellt.

Mit Eingabe der sechsstelligen eID-PIN stimmt der Bürger der Datenübertragung schließlich zu. Der Dienstanbieter kann die Echtheit und Gültigkeit des verwendeten nPA durch technische Prüfverfahren und anhand einer vom BVA zur Verfügung gestellten Sperrliste überprüfen.

II. Die Abbildung der Schriftformfunktionen unter Einsatz der Online-Ausweisfunktion

Der elektronische Identitätsnachweis ermöglicht entsprechend seinem primären Verwendungszweck insbesondere eine Abbildung der Identitätsfunktion der Schriftform. Durch die Eingabe der eID-PIN, ggf. verbunden mit einem Hinweis auf die bevorstehende Transaktion, kann auch die Warnfunktion abgedeckt werden. Die weiteren Schriftformfunktionen werden durch die eID-Funktion jedoch nicht erfüllt.

1. Einsatz der Online-Ausweisfunktion im Verwaltungsrecht

Wie unter C.I. erläutert, werden in vielen Bereichen des Verwaltungsrechts nicht alle Funktionen der Schriftform benötigt. Zur Erfüllung des Erfordernisses der ordnungsgemäßen Aktenführung etwa kommt es vorwiegend auf die Perpetuierungsfunktion an, bedarfs- und regelungsabhängig können aber auch die übrigen Schriftformfunktionen erforderlich werden.

Bezogen auf die Nutzung der Online-Ausweisfunktion bedeutet das, dass die Behörde in Abhängigkeit vom konkreten Geschäftsprozess und etwaigen Formvorschriften prüfen muss, ob und wie sie die von ihr benötigten Funktionen der Schriftform durch oder in Verbindung mit der Online-Ausweisfunktion umsetzen kann. Der elektronische Identitätsnachweis allein ist als Alternative zur qualifizierten elektronischen Signatur nicht geeignet, da er im Wesentlichen nur die Identifikationsfunktion erfüllt.

In diesem Rahmen kann die Behörde prüfen, ob sie den elektronischen Identitätsnachweis zur Erfüllung der benötigten Schriftformfunktionen einsetzen bzw. in die behördeninternen Prozesse integrieren kann. Die Erfüllung der Identitätsfunktion ist durch den Verwendungszweck des nPA unproblematisch möglich. Die Warnfunktion kann durch eine entsprechende Einbettung der Online-Ausweisfunktion in die Prozesse des jeweiligen, ggf. internetbasierten Dienstes erreicht werden. So kann der Bürger beispielsweise über einen entsprechenden schriftlichen Warnhinweis im Rahmen der jeweiligen E-Government-Anwendung informiert werden, wenn das Stadium der Vorbereitung in die Abgabe rechtsverbindlicher Erklärungen gegenüber der Behörde übergeht. Eine Abbildung der verbleibenden Funktionen der Schriftform (Abschluss-, Perpetuierungs-, Echtheits-, Verifikations- und Beweisfunktion der Schriftform) kann – sofern erforderlich – für den Bereich der Kommunikation mit staatlichen Stellen durch technisch-organisatorische Maßnahmen innerhalb der beteiligten staatlichen Stelle unter Wahrung angemessener Sicherheitsanforderungen umgesetzt werden. Hierzu muss die Nutzung der Online-Ausweisfunktion des nPA mit sicheren Prozessen im Rahmen der Datenverarbeitung der Behörden verbunden werden. Abhängig vom tatsächlichen Bedarf müssen diese Prozesse zum Beispiel sicherstellen, dass die vom Bürger übermittelten Daten (kontextbezogen etwa in Form von Anträgen oder Erklärungen) weiterhin dem betreffenden Bürger zugeordnet und im Rahmen der gesetzlich vorgegebenen Fristen geprüft werden können.

Die konkrete Prüfung, welche Funktionen der Schriftform in welchen Verwaltungsbereichen tatsächlich benötigt werden, obliegt grundsätzlich der Verwaltung und sollte – vorbehaltlich besonderer gesetzlicher Regelungen – auch bei der Verwaltung belassen werden. In Abhängigkeit vom konkreten Geschäftsprozess muss die Verwaltung sodann prüfen, wie sie die von ihr benötigten Funktionen der Schriftform in Verbindung mit der Online-Ausweisfunktion umsetzt.

2. Schriftformäquivalenz im Sozial- und Steuerrecht

Für den Bereich des Sozialrechts und des Steuerrechts gilt das zum allgemeinen Verwaltungsrecht Ausgeführte entsprechend.

3. Schriftformäquivalenz im Prozessrecht

Elektronische Erklärungen, die unter Nutzung des elektronischen Identitätsnachweises abgegeben werden, können – wie bereits dargelegt – lediglich die Identitätsfunktion und – bei entsprechender Gestaltung – die Warnfunktion der Schriftform abbilden. Aus diesem Grund ist eine Gleichsetzung der Nutzung der Online-Ausweisfunktion mit der „eigenhändigen Unterschrift“, „Unterzeichnung“ oder ähnlichem auch im Prozessrecht nicht pauschal möglich. Sowohl Perpetuierungsfunktion als auch die Notwen-

digkeit der Sicherstellung der Integrität des Erklärten über den reinen Erklärungsakt hinaus kann die Online-Ausweisfunktion nicht leisten. Beides ist im Verfahrensrecht aber regelmäßig notwendige Voraussetzung, wenn der Zustand dauerhafter Rechts- und Beweissicherheit hergestellt werden soll. Der nPA ist deshalb lediglich im Zusammenspiel mit weiteren technischen Mitteln (insbesondere sichere Kommunikationsinfrastrukturen wie z. B. De-Mail oder EGVP; durch qeS sichergestellte Überprüfbarkeit der Integrität elektronischer Dokumente) in einzelnen Fällen geeignet, als Äquivalent zur Schriftform eingesetzt zu werden.

G. Zusammenfassung/Schlussfolgerungen

1. Eine absenderbestätigte De-Mail wäre in der jetzigen Ausgestaltung durch das De-Mail-Gesetz zur Ersetzung der Schriftform im Verwaltungsrecht geeignet, wenn

– sie von einem Individual-Konto verschickt wird, für das der Absender persönlich identifiziert wurde und bei dem eine direkte Verbindung zwischen dem Endgerät des Nutzers und dem De-Mail-Provider sichergestellt ist oder wenn der Absender eine Behörde ist und nicht unmittelbar feststellbar sein muss, wer für die Behörde gehandelt hat, sowie

– eine ausreichende Warnfunktion einer absenderbestätigten De-Mail durch die Einführung einer gesonderten Schaltfläche gewährleistet wird, die zur Abgabe von Erklärungen in elektronischer Form betätigt werden muss. Um die absenderbestätigt versandte De-Mail der qeS rechtlich vollständig gleichzustellen müssten ergänzend entsprechende Beweisregelungen getroffen werden.

2. Dessen ungeachtet kann eine Ersetzung der Schriftform durch die Verwendung von De-Mail in denjenigen verwaltungsrechtlichen Fachgesetzen erfolgen, in denen ihrem Regelungszusammenhang nach auf die unter 1. genannten zusätzlichen Anforderungen an De-Mail verzichtet werden kann. Auch im Prozessrecht sind entsprechende weitere Einsatzmöglichkeiten zu prüfen.

3. Die Online-Ausweisfunktion des nPA erfüllt die Identitätsfunktion und bei entsprechender Gestaltung der zugrundeliegenden Anwendung auch die Warnfunktion der Schriftform. Alle weiteren Funktionen der Schriftform im öffentlichen Recht können grundsätzlich durch sichere behördeninterne Prozesse abgebildet werden.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333