Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)695 A

Der Landesbeauftragte
für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

Anhörung
des Innenausschusses des Deutschen Bundestages
zum Entwurf des E-Government-Gesetzes, 20.März 2013

1 Fehlendes Angebot der Ende-zu-Ende-Verschlüsselung

Nach dem vorliegenden Entwurf soll die Kommunikation zwischen Bürgerinnen, Bürgern, Unternehmen und Verwaltung mittels De-Mail abgewickelt werden können. Dieses Verfahren bietet keine Ende-zu-Ende-Verschlüsselung der übermittelten Nachrichten. Das De-Mail-Gesetz fordert:

Der akkreditierte De-Mail-Diensteanbieter (DMDA) hat sicherzustellen, dass die Kommunikationsverbindung zwischen dem Nutzer und seinem De-Mail-Konto verschlüsselt erfolgt.

Der Versand von einem DMDA zu jedem anderen DMDA muss über einen verschlüsselten gegenseitig authentisierten Kanal erfolgen.

Der Inhalt einer De-Mail-Nachricht muss vom DMDA des Versenders zum DMDA des Empfängers verschlüsselt übertragen werden.

Zwischen Nutzern und De-Mail-Diensteanbieter findet somit lediglich eine Transportverschlüsselung statt. (Die Technische Richtlinie De-Mail sieht TLS vor.) Die Diensteanbieter haben jederzeit Zugriff auf die zur Entschlüsselung nötigen Schlüssel und müssen die De-Mails zumindest kurzfristig entschlüsseln.

Das EGovG soll aber ausdrücklich Verfahren der Steuerverwaltung und der Sozialversicherung unterstützen. Insbesondere in diesen Bereichen sind Nachrichten mit hohem und sehr hohem Schutzbedarf in der Vertraulichkeit nicht selten. In diesen Anwendungsfällen ist der Einsatz von Ende-zu-Ende-Verschlüsselungsverfahren angezeigt, weil sie die Kenntnisnahme von Nachrichteninhalten bei den De-Mail-Providern technisch ausschließt.

Durch die vorgeschlagene Änderung wird erreicht, dass es keine unbefugte Offenbarung bzw. keine Datenübermittlung sein soll, wenn der De-Mail-Diensteanbieter die De-Mail kurzfristig entschlüsselt. Dieser Ansatz hat zum Ziel, dass eine De-Mail einer Ende-zu-Ende verschlüsselten Mail rechtlich gleichgestellt wird; zumindest wenn keine unbefugte Offenbarung vorliegt. Faktisch und technisch stellt diese Vorgehensweise jedoch keine Ende-zu-Ende Sicherheit her.

In den Anforderungskatalog des De-Mail-Gesetzes sollte deshalb aufgenommen werden, dass De-Mail-Diensteanbieter ihren Kundinnen und Kunden ein Ende-zu-Ende-Verschlüsselungsverfahren anbieten müssen. Die Auswahl des Verfahrens könnte dem Bundesamt für Sicherheit in der Informationstechnik (BSI) übertragen werden.

2 Pseudonyme De-Mail-Adressen zulassen

Art. 2 des Entwurfs (Änderung des De-Mail-Gesetzes) Nr. 2 b

Pseudonyme sind ein wichtiges Instrument des technischen Datenschutzes, die auch bei der Kommunikation mit Wirtschaft und Verwaltung in bestimmten Zusammenhängen sinnvoll eingesetzt werden können. Hat aber ein De-Mail-Nutzer eine Pseudonym-Adresse, so soll er unter dieser Adresse keine „absenderbestätigte De-Mail“ versenden können.

Auch eine Pseudonym-Adresse ist einem Nutzer eindeutig zuzuorden, weil der De-Mail-Diensteanbieter diese nicht doppelt vergibt. Es ist anzunehmen, dass der Klarname des Absenders aus dem Inhalt der De-Mail hervorgeht, soweit dies erforderlich ist. Trifft dies im Einzelfall

nicht zu, so kann der Nutzer über den Auskunftsanspruch nach § 16 eindeutig mit Name und Anschrift in Erfahrung gebracht werden.

Deshalb empfehle ich, den letzten Satz des Änderungsvorschlags zu § 5 Abs. 5 De-Mail-G zu streichen und absenderbestätigte De-Mails auch für pseudonyme Absenderadressen zuzulassen.

3 Qualifizierte Signatur für Zwecke der Bestätigung nach Art. 2 fragwürdig

Die in Art. 2 vorgesehene Verwendung einer qualifizierten elektronischen Signatur (QES) ist abzulehnen. Wenn der Anbieter eine De-Mail mit einer QES versieht, wird daraus bestenfalls eine Willenserklärung seinerseits - die aber inhaltlich weder zutrifft noch weiter hilft - und erst recht keine Willenserklärung des Absenders. Der Diensteanbieter kann lediglich bestätigen, dass ihm die Mail in dieser Form vorlag und der Empfänger kann prüfen, dass keine nachträglichen Veränderungen vorgenommen wurden.

Im Übrigen können nur natürliche Personen und nicht der Anbieter als juristische Person eine QES erstellen.

Für die in Art. 2 geregelte Form der Nutzung einer QES sind die im Signaturgesetz definierten Arten von Signaturen kaum nutzbar. Dies ergibt sich beispielsweise aus der Tatsache, dass die QES an eine Person und deren Handeln gebunden ist. Auch in der Begründung werden die Funktionsweisen und rechtlichen Implikationen der verschiedenen technischen Ansätze unter Berücksichtigung von ZPO, VwVfG, BGB etc nicht in der nötigen Klarheit aufgearbeitet. Die Abschnitte sollten hinsichtlich dessen, was erreicht werden soll, überdacht werden.

Es wäre sinnvoll, ein neues Instrument zu schaffen, das in einer rein ,,technischen Signatur“, Siegel genannt, zur Sicherstellung der Authentizität und Integrität besteht, welches keine Willenserklärung darstellt und die Schriftform nicht ersetzt. In Analogie zu den im Signaturgesetz vorgesehenen Instrumenten wäre für den vorgesehenen Zweck ein delegiertes Siegel mit Attribut des Absenders sinnvoll. Einem solchen Siegel könnte eine Form von (Rechts-)Verbindlichkeit unterhalb der Schriftform zukommen.

4 Zugangseröffnung missverständlich

Art. 2 (Änderung De-Mail-Gesetz) - Ziffer 3 (Änderung von § 7 Abs. 3 De-Mail-G)

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) kritisierte, dass die Veröffentlichung von Daten im Öffentlichen Verzeichnisdienst (ÖVD) mit einem besonderen Zusatz dazu führen soll, dass der Bürger damit den Zugang im Sinne des § 3a VwVfG, des § 36a Abs. 1 SGB I und § 87a Abs. 1 Satz 1 AO eröffnet. Anders als bislang würde der Bürger mit diesem Zusatz den Zugang pauschal für sämtliche Behörden eröffnen.

Dies ist kritisch zu sehen. Der Bürger sollte daher durch seinen Diensteanbieter umfassend über die Reichweite dieses Zusatzes aufgeklärt werden. Die vorgesehene Änderung sollte diese Verpflichtung ausdrücklich aufnehmen. Der Bürger muss wissen, dass er weiterhin eine spezifische Zugangseröffnung beschränkt auf einzelne Behörden vornehmen kann, dies dann aber wie bislang gegenüber jeder Behörde zu erklären hat. Ebenfalls sollte er wissen, dass nur die Veröffentlichung mit dem Zusatz die (pauschale) Zugangseröffnung zur Folge hat.

Es sollte also generell die Möglichkeit bestehen, für jede Fachanwendung einen spezifischen Zugang zu erhalten. Nur wenn ausdrücklich gewünscht, sollte der Zugang pauschal eröffnet werden.

5 Verpflichtung zur Georeferenzierung einschränken

Art. 1 § 14 Abs. 3

Die Verpflichtung zur Georeferenzierung in Registern mit Grundstücksbezug sollte nicht für die Register im Personenstands-, Melde-, Pass- und Personalausweiswesen gelten, denn die Erforderlichkeit einer Georeferenzierung ist in diesen Anwendungsfällen nicht erkennbar.

6 Formen der Einsichtnahme nach Wahl der Behörde

§ 8 des vorliegenden Gesetzentwurfs ermöglicht eine Akteneinsicht auf unterschiedlicher Art. Obwohl die Regelung kein eigenes Akteneinsichtsrecht schafft, reglementiert es deren Art und Weise jedoch

so stark, dass die Form der Akteneinsicht durch die Behörden bestimmt wird. Dieses steht im Gegensatz zum Gedanken der Informationsfreiheit. Nach § 1 Abs. 2 Satz 2 IFG hat der Antragsteller ein Wahlrecht, von der die Behörde nur aus wichtigem Grund abweichen darf.

Aus meiner Sicht sollte diesem Transparenzgedanken gefolgt und eine entsprechende Gesetzesänderung durchgeführt werden.

7 Elektronische Formulare unklar geregelt

Das Verfahren der unmittelbaren Abgabe von Erklärungen in einem elektronischen Formular unter Nutzung der eID-Funktion nach dem neuen § 3a Abs. 2 Satz 4 Nr. 1 VwVfG ist aus datenschutzrechtlicher Sicht nach wie vor unbefriedigend.

Im Gesetz werden bewusst keinerlei technische Details geregelt. Ausweislich der Begründung kann die Behörde, die entsprechende Formulare anbietet, „…durch die technische Ausgestaltung der zur Verfügung gestellten Anwendung und die eröffneten Auswahl- und Ausfüllfelder selbst steuern, welche Erklärungen abgegeben werden können und Manipulationsmöglichkeiten ausschließen.“ Nach einem sicheren Identitätsnachweis (entweder durch die eID-Funktion des nPA oder durch Identitätsfeststellung durch einen Behördenmitarbeiter vor Ort) „…muss die Behörde für eine sichere und nachvollziehbare Verknüpfung von Erklärung mit elektronischem Identitätsnachweis des Erklärenden sorgen.“ Die technische und organisatorische Ausgestaltung dieser Verfahren soll durch „verwaltungsinterne Vorschriften“ geregelt werden.

Mir erschließt sich nicht, warum solche elektronischen Verfahren eine durch Rechtsvorschrift angeordnete Schriftform ersetzen können sollen. Nach wie vor werden hier Signaturverfahren, Verfahren zur Feststellung der Identität, Authentisierungsverfahren und Verfahren zur Willenserklärung in unzulässiger Weise vermischt. Die eID-Funktion vermag die Willenserklärung, die mit dem Stellen eines Antrags verbunden ist, technisch nicht abzubilden. Nicht umsonst ist der neue Personalausweis technisch so ausgerüstet worden, dass er qualifizierte elektronische Signaturen erzeugen kann. Die eID-Funktion des Ausweises liefert hingegen Identitätsdaten hoher Qualität. Diese Identitätsdaten sind jedoch nicht mit dem Inhalt des Formulars verknüpft. Werden die Formularinhalte nachträglich verändert, so kann dies nicht mit der eID-Funktion festgestellt werden.

Zudem ist völlig unklar, wie die technische Ausgestaltung der Formularverfahren in den betreffenden Behörden aussehen soll. In der Begründung ist lediglich von einem „Baukastenmodell nach dem Vorbild des IT-Grundschutzes“ die Rede und es wird in Aussicht gestellt, dass „Mindeststandards in Form von Technischen Richtlinien“ vom BSI erarbeitet werden „könnten“. Angemessen wären aber Vorschriften, die in Struktur und Umfang mit denen des Signaturgesetzes oder des De-Mail-Gesetzes vergleichbar sind.

8 Berechtigung zum Auslesen von Identitätsdaten aus dem nPA nicht erweitern

Art. 9 (Änderung des Personalausweisgesetzes) - Ziffer 6 (Neufassung § 21 Abs. 2 Satz 1 Nr. 2 PauswG)

Die Änderung in Ziffer 6 versucht bestimmte Szenarien zu beschreiben, in denen eine Nutzung der eID möglich wird, obwohl folgend eine Übermittlung von identifizierenden Daten an Dritte - ggf. ohne Wissen des Betroffenen - erfolgen soll. Nach der Begründung zum Gesetzentwurf soll mit dieser Vorschrift die Nutzung des elektronischen Identitätsnachweises u. a. für Adresspools und Auskunfteien ausgeschlossen werden. Dafür ist aber die Gesetzesformulierung nicht klar genug, da sie auf die „nicht ausschließliche geschäftsmäßige Übermittlung“ abzielt, also eine Art Öffnungsklausel. Dadurch besteht dann aber die Gefahr, dass vor allem geschäftsmäßige Datenübermittler auf diesem Umweg Dritten verifizierte Personalausweisdaten zur Verfügung stellen können.

Ich schlage daher eine Streichung dieser Änderung vor.

9 Einsatz der eGK zur Identitätsprüfung im Sozialbereich unzulässig

(Art. 4)

Es ist vorgesehen, die elektronische Gesundheitskarte (eGK) im Geltungsbereich des Sozialgesetzbuchs als weiteres Mittel zur Identifikation neben dem neuen Personalausweis zuzulassen. Im SGB V (§ 291a) sind die Nutzungsmöglichkeiten der eGK abschließend geregelt; die

Nutzung als Identitätsnachweis ist dort nicht vorgesehen. Außerdem unterstützt die eGK keinen Identitätsnachweis, der sicherheitstechnisch mit dem des neuen Personalausweises vergleichbar wäre.

Ich empfehle daher, die eGK nicht als Identifikationsmittel zuzulassen.

10 Barrierefreiheit

(Gesetzesbegründung, S. 34)

Wegen der bisher durch den Gesetzentwurf zum EGovG nicht gewährleisteten Barrierefreiheit der darin geregelten Verfahren, ist es auch aus meiner Sicht notwendig, auf Folgendes hinweisen:
Ich unterstütze damit das Anliegen des Deutschen Blinden- und Sehbehindertenverbands e.V (DBSV), dargelegt im Schreiben vom 27.2.2013 an die Mitglieder des Innenausschusses.

Grundsätzlich ist es die beste Lösung zur Gewährleistung von Barrierefreiheit, die das BGG und das De-Mail-Gesetz ändernden Vorschriften als gesonderte Artikel in das E-Government-Gesetz einzufügen.

Hilfsweise könnte es aber auch folgende Regelung im EGovG (neuer § 16) selbst geben:

"§ 16 EGovG Barrierefreiheit

(1) Elektronische Formen der Information und Kommunikation nach diesem Gesetz müssen technisch so gestaltet sein, dass sie von behinderten Menschen grundsätzlich uneingeschränkt genutzt werden können. Elektronische Dokumente, die eine Behörde in einem Verwaltungsverfahren versendet, sind grundsätzlich barrierefrei im Sinne des § 4 des Behindertengleichstellungsgesetzes zu gestalten. Für die nach Satz 1 und 2 zu beachtenden Anforderungen gelten die Standards der zu § 11 Abs. 1 BGG erlassenen barrierefreie Informationstechnik-Verordnung in ihrer jeweils geltenden Fassung.

(2) Weitergehende Regelungen zur Barrierefreiheit, die sich aus anderen Vorschriften ergeben, bleiben unberührt."

Reinhard Dankert

Anlagen zur Information:

- Stellungnahme des BfDI vom 30.10.2012
- Handreichung des BfDI zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail

Stellungnahme des BfDI vom 31.10.2012:

EGovG, hier: Gegenäußerung der BReg zur voraussichtl. Stn des Bunderates - Ressortabstimmung

- Empfehlung des BR Nr. 10 (S. 9) zu Art. 1 (§ 2 Abs. 1 EGovG): Ich halte den Vorschlag des Bundesrates für sinnvoll. Er sollte deshalb im weiteren Gesetzgebungsverfahren geprüft werden. Es trifft zwar zu, dass nicht jede Kommunikation mit der Verwaltung verschlüsselt sein muss. Dies ist auch nicht das Ziel des Bundesratsvorschlags. In § 2 Abs. 1 EGovG geht es vielmehr darum, dass die Behörden verpflichtet sein sollen, auch verschlüsselte Dokumente entgegen nehmen zu müssen. Dies wäre ein entscheidender Schritt, um den Einsatz von Verschlüsselungsverfahren für die Bürgerinnen und Bürger sowie die Unternehmen attraktiv zu machen. Ich stimme den Bedenken der Bundesregierung allerdings insoweit zu, als sich die Verpflichtung nicht auf jede beliebige Verschlüsselung beziehen kann. Es wäre daher notwendig, hier bestimmte Standards zu setzen. Im Ergebnis sollte jedoch der Vorschlag des Bundesrates nicht abgelehnt, sondern ernsthaft geprüft werden.

- Empfehlung des BR Nr. 11 lit. b) (S. 9 f.) zu Art. 1 (§ 12 EGovG): Der Vorschlag des Bundesrates wird ausdrücklich unterstützt. Eine möglichst weitgehende Öffnung der Datenbestände der öffentlichen Hand ist im Sinne der Transparenz staatlichen Handelns notwendig. Die angeregte Verankerung verbindlicher Veröffentlichungspflichten sollte aber besser in § 11 IFG erfolgen und nicht im EGovG.

- Empfehlung des BR Nr. 14 (S. 12) zu Art. 1 (§ 14 Abs. 3 - neu - EGovG): Die Verpflichtung zur Georeferenzierung soll nicht für die Register im Personenstands-, Melde-, Pass- und Personalausweiswesen gelten. Dem Vorschlag des Bundesrates wird zugestimmt. Jedenfalls für die Pass- und Personalausweisregister ist in der Tat keine Erforderlichkeit für eine Georeferenzierung erkennbar.

- Empfehlung des BR Nr. 15 (S. 13) zu Art. 1 (§ 15 Abs. 2 Satz 6 - neu - EGovG): Dem Vorschlag des BR wird zugestimmt. Zwar ist es richtig, dass bei einer Veröffentlichung datenschutzrechtliche Bestimmungen zu beachten sind. Die meisten Vorschriften zur Veröffentlichungspflichten sind aber nach wie vor auf die Publikation in gedruckten Werken zugeschnitten und nicht auf die elektronische Veröffentlichung im Internet. Die Risiken einer Verletzung des Persönlichkeitsrechts sind jedoch bei einer Veröffentlichung im Internet aufgrund der weltweiten Verfügbarkeit und der leichteren Auswertbarkeit digitalisierter Daten deutlich höher. Insofern halte ich es für einen sachgerechten Vorschlag, hier eine zeitliche Begrenzung zu ermöglichen.

- Empfehlung des BR Nr. 16 (S. 13) zu Art. 2 (De-MailG): Der BR bittet zu prüfen, ob durch eine Änderung des Gesetzes eine konkludente Zugangseröffnung für den "Rückkanal" (Behörde antwortet auf eine De-Mail des Bürgers) konstruiert werden kann. In der Gegenäußerung soll auf die allgemeine Zugangseröffnung durch den ÖVD sowie die Verkehrsanschauung verwiesen werden. Schon die generelle Zugangseröffnung gegenüber allen Behörden durch die Veröffentlichung im ÖVD ist kritisch zu sehen, wie der BfDI bereits in seiner Stellungnahme vom 01.08.2012 ausgeführt hat. Darauf weise ich insoweit erneut hin. Dementsprechend ist eine konkludente Zugangseröffnung für den

"Rückkanal" erst recht abzulehnen.

- Empfehlungen des BR Nr. 22 und 23 (S. 17 ff.) zu Art. 3 Nr. 3 (§ 27a VwVfG): Bei einer öffentlichen Bekanntmachung über das Internet ist in jedem Falle zu beachten, dass im Einzelfall personenbezogene Daten betroffen sein können und in diesem Falle die datenschutzrechtlichen Bestimmungen zu beachten wären (die insoweit gem. § 1 Abs. 4 BDSG Vorrang hätten). Dies sollte bei der Prüfung des § 27a VwVfG berücksichtigt werden.

- Empfehlung des BR Nr. 24 (S. 19) zu Art. 9 (§§ 10 Abs. 1 und 11 Abs. 4 PAuswG): Der BR bittet zu prüfen, ob weitere Schriftformerfordernisse im PAuswG gestrichen werden könnten. Jedenfalls hinsichtlich für den Bürger besonders relevanter Erklärungen, in der die Unterschrift auch eine Warnfunktion hat, sollte auf die Schriftform nicht verzichtet werden. Dies gilt insbesondere für die Erklärungen im Zusammenhang mit der Abgabe der Fingerabdrücke. Hier ist der Bürger umfassend, und zwar im unmittelbaren Zusammenhang mit der Abgabe, aufzuklären. Sofern er sich dennoch für eine Speicherung entscheidet, sollte er diese Entscheidung mit seiner Unterschrift dokumentieren.

- Empfehlung Nr. 25 (S. 21) zu Art. 9 (§ 21 Abs. 2 Nr. 2a PAuswG): Dem Formulierungsvorschlag des Bundesrates wird zugestimmt. Die aktuelle Entwurfsfassung des § 21 Abs. 2 Nr. 2a ist das Ergebnis eines Kompromisses. Die vom BR vorgeschlagene Fassung entspricht in seiner Intention den vom BfDI im Laufe der Ressortabstimmung vorgeschlagenen Fassungen.

Mit freundlichen Grüßen
Im Auftrag

Sven Hermerschmidt
--
Referat I
Grundsatzfragen; nicht-öffentlicher Bereich
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Verbindungsbüro
Friedrichstr. 50
10117 Berlin
Tel: +49-30-187799-115
Fax: +49-30-187799-552
Email: sven.hermerschmidt@bfdi.bund.de (persönlich) oder ref1@bfdi.bund.de (Referat)
Internetadresse: www.datenschutz.bund.de

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, 1. März 2013

Handreichung
zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail

Die Handreichung soll die Nutzer von De-Mail für die datenschutzrechtlichen Aspekte bei der Versendung besonders schützenswerter Daten mittels De-Mail sensibilisieren. Sie soll Hinweise für einen datenschutzgerechten Versand dieser Daten mittels De-Mail unter Berücksichtigung der Möglichkeit einer Ende-zu-Ende-Verschlüsselung geben, um damit zu einer rechtssicheren und weiten Verbreitung von De-Mail-Diensten beizutragen.

Am 3. Mai 2011 ist das De-Mail-Gesetz in Kraft getreten. Auf Grundlage dieses Gesetzes können sich Unternehmen akkreditieren lassen, um De-Mail-Dienste anzubieten. De-Mail-Dienste sind nach § 1 Abs. 1 De-Mail-Gesetz Telekommunikationsdienste auf einer elektronischen Plattform, die eine sichere, vertrauliche und nachweisbare Kommunikation für jedermann im Internet gewährleisten sollen. Die De-Mail ist letztlich eine besondere Form der E-Mail. Sie soll ohne zusätzliche Hard- und Software genauso einfach bedienbar sein, aber die Nachteile der E-Mail ausgleichen. Eine E-Mail kann nämlich mit geringem technischem Aufwand abgefangen, mitgelesen und verändert werden.

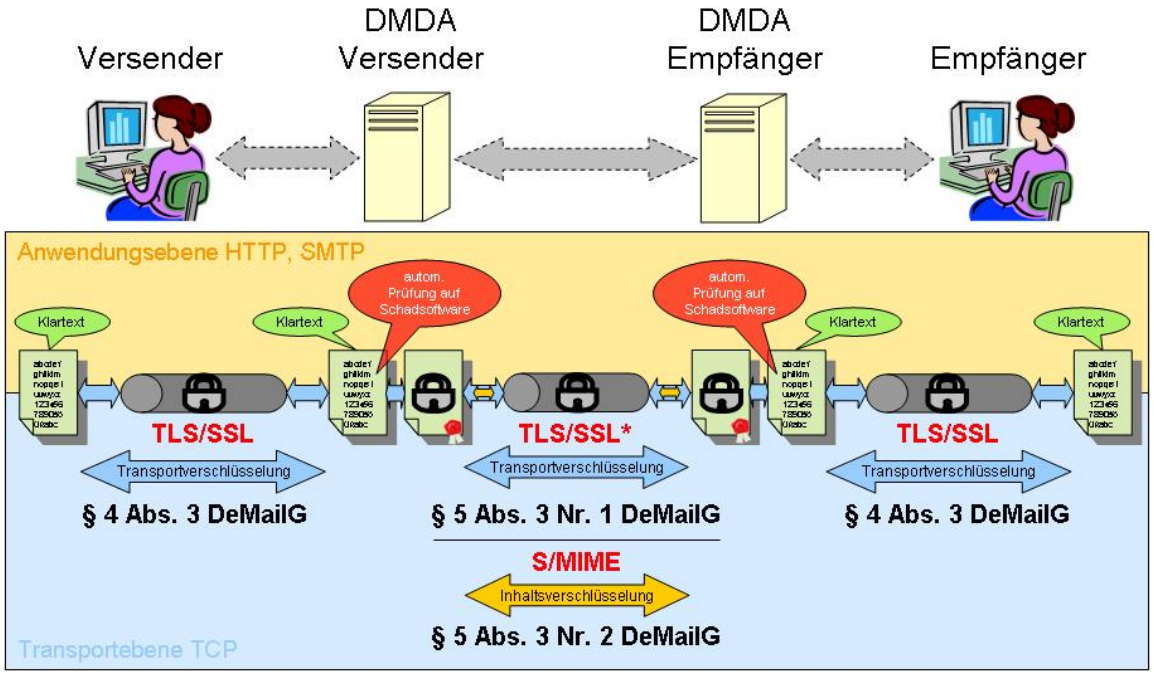
Das De-Mail-Gesetz stellt einerseits Anforderungen an Datenschutz und Datensicherheit beim De-Mail-Diensteanbieter (DMDA) und regelt andererseits, wie De-Mail für die rechtssichere elektronische Kommunikation eingesetzt werden kann. Dies bedingt einige Besonderheiten im Vergleich zur Nutzung von E-Mail-Diensten, so z.B. eine eindeutige Identifizierung vor der erstmaligen Nutzung von De-Mail. De-Mail bietet die Gewähr dafür, dass der Absender einer De-Mail zweifelsfrei ermittelt werden kann. Absende- und Eingangsbestätigungen, die mit einer qualifizierten elektronischen Signatur des DMDA versehen werden, bieten den sicheren Nachweis, dass die De-Mail versendet wurde und eingegangen ist. Schließlich wird die Nachricht durch den Anbieter transport- und inhaltsverschlüsselt.

Das De-Mail-Gesetz fordert:

- Der akkreditierte DMDA hat sicherzustellen, dass die Kommunikationsverbindung zwischen dem Nutzer und seinem De-Mail-Konto verschlüsselt erfolgt.
- Der Versand von einem DMDA zu jedem anderen DMDA muss über einen verschlüsselten gegenseitig authentisierten Kanal erfolgen.
- Der Inhalt einer De-Mail-Nachricht muss vom DMDA des Versenders zum DMDA des Empfängers verschlüsselt übertragen werden.

Die technischen Details lassen sich wie folgt zusammenfassen:

- Die Nachricht vom Versender an seinen DMDA und weiter vom DMDA des Empfängers an den Empfänger ist auf der Transportebene jeweils einfach durch Transportverschlüsselung gesichert (TCP + SSL/TLS). Die Authentisierung des Clients erfolgt automatisch mittels SSL-Handshake. Eine zertifikatsbasierte Clientauthentifizierung wird optional unterstützt.
- Die Nachricht ist zwischen dem DMDA des Versenders und dem DMDA des Empfängers doppelt gesichert: auf Anwendungsebene durch Inhaltsverschlüsselung und Signatur der Nachricht (S/MIME) sowie auf Transportebene durch Transportverschlüsselung (TCP + implizites1 SSL/TLS). Eine gegenseitige Clientauthentisierung muss zwingend zertifikatsbasiert erfolgen.
- Die Transportverschlüsselung (TLS) ist eine Punkt-zu-Punkt-Verschlüsselung (SSL-Handshake), weshalb die Nachricht nach dem Versand wieder unverschlüsselt vorliegt. Auf Transportebene liegt die Nachricht also in einem zufälligen Bitmuster vor, jedoch wäre sie auf Anwendungsebene ohne weiteres im Klartext zu lesen.
- Die Inhaltsverschlüsselung (S/MIME) ist eine Ende-zu-Ende-Verschlüsselung, wird aber gemäß TR De-Mail nur zwischen zwei DMDA gefordert.



§ 3 Abs. 4 Nr. 4 De-Mail-Gesetz sieht vor, dass der DMDA die De-Mail auf Befall mit Schadsoftware überprüfen muss. Vor dem Versand der Nachricht an den DMDA des Empfängers liegt diese beim DMDA des Versenders unverschlüsselt vor, so dass er sie zu diesem Zeitpunkt auf Schadsoftwarebefall hin prüfen kann. Anschließend leitet er die Nachricht zusätzlich zur Transportverschlüsselung inhaltsverschlüsselt an den DMDA des Empfängers weiter. Ist die Nachricht beim DMDA des Empfängers eingegangen, wird die Inhaltsverschlüsselung aufgehoben und die Nachricht wiederum auf Schadsoftwarebefall hin geprüft. Abschließend wird die Nachricht verschlüsselt im Postfach des Empfängers abgelegt. Nach jeder Prüfung wird die Nachricht in den Metadaten mit einem Hinweis versehen, ob die Überprüfung zu einem Befund geführt hat. Dieser Prüfprozess erfolgt zwar automatisiert auf Servern in einem Rechenzentrum des DMDA, das den Vorgaben des BSI entspricht. Zudem gibt es weitere technische und organisatorische Maßnahmen, die einen Zugriff durch einen Innen- wie auch einen Außentäter verhindern sollen. Gleichwohl besteht ein Restrisiko, dass insbesondere Administratoren des Anbieters vom Nachrichteninhalt Kenntnis nehmen.

Im Gegensatz dazu stellt die Ende-zu-Ende-Verschlüsselung eine durchgängige Verschlüsselung zwischen Versender und Empfänger dar und bietet sich daher für eine Versendung besonders schutzbedürftiger Daten an. Dies wird vom De-Mail-

Gesetz jedoch nicht gefordert. Für den DMDA ergeben sich dementsprechend keine Pflichten. Er darf den Versand Ende-zu-Ende-verschlüsselter Nachrichten lediglich nicht verhindern. Faktisch bedeutet dies, dass sich die Nutzer selbst um die Installation und Nutzung einer Verschlüsselungssoftware kümmern müssen. Eine Prüfung auf Schadsoftware kann der DMDA dann allerdings nicht durchführen. Problematisch ist zudem, dass Nachrichten nur dann verschlüsselt versendet werden können, wenn auch der Empfänger eine entsprechende Kryptografiesoftware einsetzt. Dies führt zu Verunsicherungen und Erschwernissen, die sich hätten vermeiden lassen, wenn die Ende-zu-Ende-Verschlüsselung zu den mit De-Mail bereitgestellten Standardmaßnahmen gehören würde.

Da die bisher akkreditierten DMDA für den Privatanwender bislang nur den Zugang per Web-Client ermöglichen, ist eine Ende-zu-Ende-Verschlüsselung für diesen derzeit kaum praktikabel. Der Versender muss die zu übermittelnde Nachricht auf seinem lokalen Rechner erstellen und mit einer Kryptografiesoftware verschlüsseln. Danach meldet er sich über den Web-Client an seinem De-Mail Konto an, erzeugt eine leere „Pseudo“-De-Mail und hängt dieser per Upload die verschlüsselte Datei an. Wirtschaftsunternehmen und die öffentliche Verwaltung haben es hier einfacher, da die Anbindung an De-Mail über ein Gateway erfolgt, d.h. im Firmen- bzw. Behördennetzwerk können normale E-Mail-Clients wie Outlook oder Lotus Notes genutzt werden, die von Hause aus eine Verschlüsselung unterstützen, so dass diese weitestgehend automatisiert erfolgen kann.

Es ist ein Grundsatz des Datenschutzes, dass bei der elektronischen Übertragung personenbezogener Daten die Integrität, Authentizität und Vertraulichkeit der Daten sichergestellt sein muss. Je schützenswerter ein Datum ist, desto strenger sind die technisch-organisatorischen Maßnahmen, die die verantwortliche Stelle einhalten muss. Bei bestimmten personenbezogenen Daten wie zum Beispiel Gesundheitsdaten, spielt besonders die Vertraulichkeit eine große Rolle. Unbefugte sollen in keinen Fall Kenntnis von diesen Daten erhalten. Bei der elektronischen Kommunikation wird die Vertraulichkeit dadurch gewährleistet, dass die Nachricht und ihre Anhänge mit einer geeigneten Software verschlüsselt werden. Betroffen sind hiervon alle besonders schutzbedürftigen personenbezogenen Daten, also solche, die potentiell eine besondere Sensibilität aufweisen. Dies gilt etwa für personenbezogene Daten an deren Verarbeitung und Nutzung besondere gesetzliche Anforderungen gestellt werden, wie z.B. die so genannten besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG oder die dem Sozialdatenschutz unterfallenden personenbezogenen Daten. Welche Schutzmaßnahmen für diese Daten angemessen sind, ergibt sich allerdings nicht automatisch, sondern bedarf einer Prüfung im Einzelfall, die im Folgenden weiter ausgeführt wird.

Mangels entsprechender gesetzlicher Vorgaben im De-Mail-Gesetz sind nicht die DMDA, sondern die Versender von De-Mails für die Beachtung datenschutzrechtlich angemessener Verfahren verantwortlich. Um ein angemessenes Schutzniveau bei der Versendung besonders schutzbedürftiger personenbezogener Daten (z.B. Sozialdaten oder Daten die Rückschlüsse auf den Gesundheitszustand einzelner Betroffener zulassen) mittels De-Mail zu gewährleisten, ist aus datenschutzrechtlicher Sicht eine Ende-zu-Ende-Verschlüsselung grundsätzlich erforderlich. Die Vorgaben des De-Mail-Gesetzes, die Technische Richtlinie des BSI nach § 18 Abs. 2 De-Mail-Gesetz und der Kriterienkatalog des BfDI gemäß § 18 Abs. 3 Nr. 4 De-Mail-Gesetz machen zwar deutlich, dass bei De-Mail das Datenschutz- und Datensicherheitsniveau im Vergleich zum E-Mail-Versand erheblich höher ist. Trotzdem müssen über diesen Mindeststandard hinaus beim Versand besonders schutzbedürftiger Daten grundsätzlich zusätzliche Schutzvorkehrungen getroffen werden.

Ob eine Ende-zu-Ende-Verschlüsselung im Einzelfall die datenschutzrechtlich angemessene Sicherungsmaßnahme darstellt, orientiert sich an dem konkreten Schutzbedarf der Daten. Dieser ist zunächst anhand der Grundschutzmethodik des BSI von der datenverarbeitenden Stelle festzustellen:

- Bei einer Schutzbedarfsfeststellung ist grundsätzlich danach zu fragen, welcher Schaden entstehen kann, wenn die Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit verletzt werden. Es muss also gefragt werden, welcher Schaden eintritt, wenn vertrauliche Informationen unberechtigt zur Kenntnis genommen oder weitergegeben werden (Verletzung der Vertraulichkeit), die Korrektheit der Informationen und die Funktionsweise von Systemen nicht mehr gegeben ist (Verletzung der Integrität) oder autorisierte Benutzer am Zugriff auf Informationen und Systeme behindert werden (Verletzung der Verfügbarkeit). Dabei wird zwischen den Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ unterschieden. Der Schaden, der von einer Verletzung der Grundwerte ausgehen kann, kann sich auf verschiedene Schadensszenarien beziehen:
    - Verstöße gegen Gesetze, Vorschriften oder Verträge,
    - Beeinträchtigungen des informationellen Selbstbestimmungsrechts,
    - Beeinträchtigungen der persönlichen Unversehrtheit,
    - Beeinträchtigungen der Aufgabenerfüllung,
    - negative Außenwirkung oder
    - finanzielle Auswirkungen.

- Beim Schutzbedarf „normal“ sind die Schadensauswirkungen begrenzt und überschaubar. Beim Versand von Daten mit dem Schutzbedarf „normal“ ist eine Ende-zu-Ende-Verschlüsselung dann nicht notwendig.

- Beim Schutzbedarf „hoch“ können die Schadensauswirkungen beträchtlich sein. Beim Versand von Daten mit dem Schutzbedarf „hoch“ ist eine Ende-zu-Ende-Verschlüsselung grundsätzlich erforderlich. Auf sie kann jedoch dann verzichtet werden, wenn die datenverarbeitende Stelle anhand einer Risikoanalyse zu dem Ergebnis kommt, dass sie aufgrund der getroffenen technischen und organisatorischen Sicherheitsmaßnahmen das Restrisiko im Bereich des Versenders als vertretbar bewertet. Versender und Empfänger müssen sich aber auf jeden Fall an ihrem Konto im Sinne des § 4 Abs. 1 Satz 2 De-Mail-Gesetz sicher anmelden.

- Beim Schutzbedarf „sehr hoch“ können die Schadensauswirkungen bei unberechtigtem Zugriff ein existentiell bedrohliches Ausmaß erreichen. Beim Versand von Daten mit dem Schutzbedarf „sehr hoch“ ist eine Ende-zu-Ende-Verschlüsselung zwingend notwendig.

- Bei der Schutzbedarfsanalyse ist Folgendes zu beachten:

    - Die Einstufung des jeweiligen personenbezogenen Datums kann je nach Kontext, in dem das Datum verwendet wird, unterschiedlich sein. So ist beispielsweise der Schutzbedarf einer Adresse im Regelfall behördlicher Anwendungen normal oder hoch. Befindet sich die betroffene Person aber in einem Zeugenschutzprogramm, ist der Schutzbedarf sehr hoch und die Daten dürften nur mit Ende-zu-Ende-Verschlüsselung übertragen werden.

    - Sozial- und Steuergeheimnisdaten sind zwar nach dem Gesetz insofern als besonders schützenswert eingestuft, als ihre Verarbeitung zum Teil besonderen Restriktionen unterliegt. Allerdings bedeutet dies nicht, dass sämtliche Sozial- und Steuergeheimnisdaten Ende-zu-Ende-verschlüsselt werden müssen. Die Tatsache, dass eine Person beispielsweise bei einer bestimmten gesetzlichen Krankenkasse versichert ist, ist im Regelfall kein besonders schützenswertes Datum.

    - Gesundheitsdaten unterliegen dagegen in aller Regel dem Schutzbedarf „sehr hoch“. Dies gilt wiederum auch unabhängig vom Kontext als Sozialdatum. Auch die Angabe von besonderen Belastungen bei

Krankheitsaufwendungen im Zusammenhang mit einer Einkommenssteuererklärung sind besonders schutzbedürftig, auch wenn Steuergeheimnisdaten nicht automatisch Ende-zu-Ende-verschlüsselt werden müssen.

Neben der Schutzbedarfsanalyse muss für eine Einschätzung der notwendigen Sicherheitsmaßnahmen beim Versand besonders schutzbedürftiger Daten auch berücksichtigt werden, wer Versender und Empfänger der De-Mail ist:

- Versenden Behörden oder andere Institutionen besonders schutzbedürftige personenbezogene Daten unmittelbar an den Betroffenen, richtet sich die Verpflichtung zur Ende-zu-Ende-Verschlüsselung grundsätzlich nach dem im Wege der Schutzbedarfsanalyse ermittelten Schutzbedarf der Daten. Daneben muss der Versender vor dem Versand das Einverständnis des potentiellen Empfängers einholen[1]. Dies sollte mindestens einmalig für alle diesen Transportweg betreffenden Kommunikationsvorgänge erfolgen. Zusätzlich muss für den Versand besonders schutzbedürftiger Daten mittels De-Mail an den Betroffenen eine individuelle Zugangseröffnung vorliegen[2]. Dies gilt insbesondere für eine differenzierte Betrachtung bei der Zugangseröffnung gegenüber Behörden. Der Bürger sollte die Möglichkeit haben, den Zugang differenziert nach einzelnen Behörden zu gestalten.

- Versenden Behörden oder andere Institutionen wie etwa gesetzliche Krankenkassen, die mit besonders schutzbedürftigen personenbezogenen Daten Dritter umgehen, solche Daten untereinander, muss die Nachricht im Ergebnis auch ohne ein Schutzbedarfsanalyse Ende-zu-Ende verschlüsselt werden. Betrachtet man den Versand einzelner Nachrichten, würde eine Schutzbedarfsanalyse an sich zu dem Ergebnis kommen, dass in bestimmten Fällen (z.B. beim Schutzbedarf „normal“) eine Ende-zu-Ende-Verschlüsselung nicht erforderlich ist. Hier muss aber berücksichtigt werden, dass im Falle eines unberechtigten Zugriffs beim DMDA durch die Vielzahl der versandten bzw. empfangenen Daten ein erhöhtes Angriffsrisiko und Schadenspotential vorliegt (Kumulationseffekt). Außerdem kann der Betroffene nicht entscheiden, auf welche Weise seine Daten versandt werden. Die Tatsache, dass der Betroffene in diesen Fällen keinen Einfluss auf die Ausgestaltung der De-Mail-Nutzung nehmen kann, darf nicht zu einer Absenkung des Datenschutzniveaus bei der Versendung

[1] Dies gilt generell für den Versand personenbezogener Daten, also auch für solche, die als nicht besonders schutzbedürftig eingestuft werden.
[2] Vgl. Fußnote 1.

besonders schutzbedürftiger Daten mittels De-Mail führen. Schließlich kann man davon ausgehen, dass solche Einrichtungen den De-Mail-Dienst über ein Gateway nutzen können und daher eine Ende-zu-Ende-Verschlüsselung in diesen Fällen mit vertretbarem technischen Aufwand möglich ist. Die Verpflichtung gilt unabhängig von der Größe der Einrichtung und unabhängig davon, ob eine gesetzliche Pflicht zur Datenverarbeitung besteht. Letztlich führt die einheitliche Behandlung alle Nachrichteninhalte in diesem Kommunikationsverhältnis auch zur einer handhabbaren Anwendung für Versender und Empfänger.

Der Entwicklungsstand der Technik und die tatsächliche Verfahrensweise im Umgang mit De-Mail muss beobachtet werden. Daraus können sich in Zukunft neue oder andere Anforderungen des Datenschutzes an die Verwendung von De-Mail und die Verschlüsselung ergeben. Die DMDA werden aufgefordert, leicht handhabbare Verschlüsselungsoptionen für die Nutzer zu entwickeln. Dies kann auch Datenschutzverstöße aufgrund einer fehlerhaften Schutzbedarfsfeststellung der verantwortlichen Stelle verhindern.

Schließlich müssen auch die internen Verfahrensabläufe bei der versendenden sowie bei der empfangenden Stelle betrachtet werden, also z.B. die Verknüpfung des Fachverfahrens mit dem De-Mail-Postfach und interne Zugriffsberechtigungen in den Unternehmen und Behörden. Auch diese müssen datenschutzkonform ausgestaltet sein und die Sicherheit der Daten gewährleisten.