Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)173 A

Dipl. Informatiker Werner Hülsmann:

Stellungnahme für den Innenausschuss des Deutschen Bundestages zum Gesetzentwurf zur Regelung von De-Mail-Diensten

Inhaltsverzeichnis

Dipl. Informatiker Werner Hülsmann – Obere Laube 48 – D-78462 Konstanz – Tel.: 07531 / 365 90-56, mobil: 0179 / 46 86 484
E-Mail: werner@fiff.de – URL: www.fiff.de – www.datenschutzconsulting.info

1 Vorbemerkung

Der Autor wurde am 31. Januar 2011 als Sachverständiger des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages zum Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Regelungen von De-Mail-Diensten und zur Änderung weiterer Vorschriften" (BT-Drucksachen 17/3638, 17/414) am 07. Februar 2011 in Berlin eingeladen. Auf Grund der Kürze der zur Verfügung stehenden Zeit – eine Abgabe der schriftlichen Stellungnahme wurde zu Donnerstag, 03. Februar 2011 erwartet – kann die nachfolgende Stellungnahme nur die wichtigsten Punkte anreißen und erhebt insoweit keinen Anspruch auf Vollständigkeit.

2 Zusammenfassung

Grundsätzlich ist es zu begrüßen, dass durch das De-Mail-Vorhaben die Vertraulichkeit und Verifizierbarkeit (Authentizität der Absende- und Empfangsadresse, Integrität des Inhalts) gefördert und die Kommunikation zwischen Bürger/innen und Verwaltung vereinfacht werden soll. Allerdings sind im Gesetzgebungsverfahren noch wichtige Korrekturen und Änderungen vorzunehmen.

2.1 Nicht zu erfüllende Erwartungen

In der De-Mail-Broschüre des Bundesministeriums für Inneres (Stand Dezember 2010) werden allerdings Erwartungen an De-Mail geweckt, die entweder nicht von De-Mail erfüllt werden oder unabhängig von De-Mail sind. Da mit diesen Aussagen an vielen Stellen für das De-Mail-Verfahren, wie es sich aus dem aktuellen Gesetzesentwurf ergibt, geworben wird, werden an dieser Stelle diese nicht mit De-Mail zu erfüllenden Erwartungen erörtert.

- Die Nutzung von De-Mail spare Geld: Solange die Preise für den Versand (und evtl. Empfang) von De-Mails nicht feststehen, können keinerlei Aussagen zu möglichen Kosteneinsparungen für Bürger/innen getroffen werden. Da heutzutage der FAX-Versand bei einer Festnetzflatrate kostenlos ist, sind nur gegenüber Briefen überhaupt Kosteneinsparungen möglich. Die Erfahrungen mit dem ePost-Brief zeigen allerdings, dass günstigere Versandkosten beim elektronischen Versand keineswegs selbstverständlich sind.
- De-Mail schütze vor SPAM und vor Phishing: Dies würde nur dann gelten, wenn alle E-Mails, die nicht von einem verifizierten Absender kommen vom Provider automatisch gelöscht würden. Dies wäre aber fatal, da De-Mail zu keiner Zeit eine 100%-ige Verbreitung haben wird und somit viele erwünschte E-Mails – nicht nur aus dem Ausland – gelöscht würden.

Dipl. Informatiker Werner Hülsmann – Obere Laube 48 – D-78462 Konstanz – Tel.: 07531 / 365 90-56, mobil: 0179 / 46 86 484
E-Mail: werner@fiff.de – URL: www.fiff.de – www.datenschutzconsulting.info

- De-Mail unterstütze und fördere den (Selbst-)Datenschutz: Da De-Mail-Adressen nur nach einer Verifizierung der Person vergeben werden, sind echte anonyme oder pseudonyme E-Mail-Nutzungen nicht möglich. Der Provider kennt den/die Inhaber/in eines Pseudonyms und ist technisch auch in der Lage auf die Inhalte der De-Mails zuzugreifen. Zudem werden nach dem Entwurf Provider nicht verpflichtet, Pseudonyme De-Mail-Adressen zu vergeben.
- Die Nutzung der Ende-zu-Ende-Verschlüsselung werde erheblich vereinfacht: De-Mails sind gerade nicht Ende-zu-Ende-verschlüsselt. Vielmehr werden sie vom De-Mail-Provider des Absenders als auch vom De-Mail-Provider des Empfängers für einen Virencheck entschlüsselt und dann wieder verschlüsselt. Wenn keine De-Mail-Plugins für gängige Mailprodukte wie Thunderbird, Outlook, Outlook-Express und andere zur Verfügung gestellt werden, ist der Aufwand für eine Ende-zu-Ende-Verschlüsselung höher als bei den bisher gängigen Verfahren wie PGP und GnuPG, da die Inhalte der Mail von dem/der Absender/in erst verschlüsselt werden müssen, bevor sie im De-Mail-Webfrontend eingegeben werden können. Umgekehrt muss der/die Empfänger/in den Ende-zu-Ende-verschlüsselten Inhalt erst aus der Mail herauskopieren und dann entschlüsseln. Es wäre allerdings für die De-Mail-Dienstleister möglich, bei entsprechender rechtlicher Verpflichtung, die Ende-Zu-Ende-Verschlüsselung bei der De-Mail-Nutzung zu integrieren und damit für die De-Mail-Nutzer/innen zu vereinfachen

2.2 Datenschutz und Datensicherheit

Zur Sicherstellung des Datenschutzes ist es erforderlich, dass die akkreditierten Dienstleister verpflichtet werden, natürlichen Personen mehrere Pseudonyme anzubieten. Ohne diese Verpflichtung läuft die Regelung zu den Pseudonymen ins Leere. Bei den Aufklärungs- und Informationspflichten nach § 9 sind Informationen über die Nutzung von Pseudonymen zu ergänzen. Die Änderungsvorschläge h und m bb) des Änderungsantrags vom 21. Januar 2011 der Regierungsfraktionen sind aus Datenschutzsicht zu begrüßen und sollten daher umgesetzt werden.

2.3 Brief, Post- und Fernmeldegeheimnis

Zur Sicherstellung des Brief- Post und Fernmeldegeheimnisses ist es den De-Mail-Nutzern auf einfache Art und Weise zu ermöglichen, eine Ende-zu-Ende-Verschlüsselung zu aktivieren. De-Mail bietet selbst keine Ende-zu-Ende-Verschlüsselung an, sondern lediglich eine Transportverschlüsselung. De-Mailanbieter haben zur Filterung der De-Mails auf das Vorhandensein von Schadprogrammen und Viren auf ihren Servern Zugriff auf die versandten und empfangenen De-Mails. Das De-Mail-Verfahren genügt damit nicht den Ansprüchen an das Brief, Post- und Fernmeldegeheimnis nach Art. 10 Abs. 1 GG.

Dipl. Informatiker Werner Hülsmann – Obere Laube 48 – D-78462 Konstanz – Tel.: 07531 / 365 90-56, mobil: 0179 / 46 86 484
E-Mail: werner@fiff.de – URL: www.fiff.de – www.datenschutzconsulting.info

Zudem fehlen besondere Schutzregeln, die die besonderen Risiken des Drittzugriffs auf die bei den De-Mail-Anbietern anfallenden und zum Teil in der Dokumentenablage über längere Zeiträume vorgehaltenen E-Mails und Anhänge ausreichend berücksichtigen.

2.4 Verbraucherschutz

Zur Förderung des Wettbewerbs muss sichergestellt werden, dass De-Mail-Adressen leicht von einem Anbieter zum nächsten portierbar sind. Daher sollten sie einheitlich nach dem Schema vorname.nachname.xxxxx@de-mail.de gebildet werden.

Die technischen Regelungen zu Versands- und Empfangszertifikaten walzen die Beweislast für den Nichterhalt in zu großem Umfang auf Bürger/innen ab, deren Widerspruchsmöglichkeiten gegenüber einem komplexen technischen System begrenzt sind.

Die Zustellfiktion des Verwaltungsverfahrensgesetzes wird unnötigerweise verschärft (Wochenende und Feiertage zählen mit, drei Tage nach Versand vom Behördenserver zählt eine Nachricht in jedem Fall als zugestellt, mit dem Login des Nutzers wird eine Abholbestätigung bereits versandt).

Das Porto für De-Mails ist bisher unklar, es gibt keine Rahmensetzung für den Wettbewerb.

Die Belange des Verbraucherschutzes sollten bereits bei der Akkreditierung berücksichtigt werden.

2.5 Verhältnis BürgerInnen/Staat:

De-Mail ist kein transparentes System und weit entfernt von Open Source-Lösungen und „Open Government“. Es wirkt in den gesetzlichen Regelungen eher wie ein reines Effizienzinstrument für behördliche Kommunikation, das Bürger/innen.

Die fehlende Bürger/innenorientierung ist kontraproduktiv und schadet der Akzeptanz in der Bevölkerung.

2.6 Gesamtkonzept:

Bereits bestehende Lösungen werden nicht integriert, darunter das Signaturgesetz und das elektronische Verwaltungs- und Verfahrenspostfach. In der Konkurrenzsituation zwischen E-Postbrief und De-Mail bleibt für Bürgerinnen und Bürger unklar, wie sie auf die beste Weise elektronisch mit dem Staat interagieren können.

3 Zu den Regelungen im Einzelnen

Bezüglich der Nichterwähnung einzelner Regelungen verweise ich auf die Vorbemerkung. Die Stellungnahme zu einzelnen Regelungen darf allerdings nicht davon

Dipl. Informatiker Werner Hülsmann – Obere Laube 48 – D-78462 Konstanz – Tel.: 07531 / 365 90-56, mobil: 0179 / 46 86 484
E-Mail: werner@fiff.de – URL: www.fiff.de – www.datenschutzconsulting.info

ablenken, dass einige wesentliche Änderungen im Bereich Daten- und Verbraucherschutz (s.o.) erforderlich sind.

3.1 Zum Änderungsantrag der Regierungsfraktionen vom 21. Januar 2011 (Ausschussdrucksache 17(4)266)

3.1.1 Zu Ziffer 1

3.1.1.1 Zu Buchstabe a)

Die Änderung wird befürwortet

3.1.1.2 Zu Buchstabe b)

Die Änderung ist akzeptabel.

3.1.1.3 Zu Buchstabe c)

Diese Änderung führt zu einem verständlicherem Gesetzestext und ist daher zu begrüßen.

3.1.1.4 Zu Buchstaben d) - g)

Diese Änderungen werden befürwortet. Ergänzend zu Buchstabe f) sollte auch der Hinweis auf die Möglichkeit der Nutzung von pseudonymen De-Mail-Adressen in der Information enthalten sein.

3.1.1.5 Zu Buchstabe h)

Diese Änderung ist zur Wahrung des Datenschutzes der De-Mail-Nutzer/innen erforderlich.

3.1.1.6 Zu Buchstabe i)

Auch diese Änderung sollte aus Gründen des Datenschutzes umgesetzt werden.

3.1.1.7 Zu Buchstabe j)

Hier empfiehlt sich das Wort „Zertifikate“ nicht nur durch „Testate“ sondern durch „Testate und Zertifikate“ zu ersetzen.

3.1.1.8 Zu Buchstabe k)

Diese Änderung wird befürwortet.

3.1.1.9 Zu Buchstabe l)

Hier sind nicht nur Vertreter/innen von Gesamtverbänden sondern auch Vertreter/innen von Verbraucherschutzverbänden und Datenschutzorganisationen wie auch von Nutzer/innen eingebunden werden, damit die Verbraucher- und Datenschutzbelange ausreichend Gehör finden und um eine möglichst große Bürger/innenbeteiligung zu ermöglichen.

Dipl. Informatiker Werner Hülsmann – Obere Laube 48 – D-78462 Konstanz – Tel.: 07531 / 365 90-56, mobil: 0179 / 46 86 484
E-Mail: werner@fiff.de – URL: www.fiff.de – www.datenschutzconsulting.info

3.1.1.10 Zu Buchstabe m)

Die Änderung zu aa) ist eine Folgeänderung. Die Änderung zu bb) ist erforderlich, um Verstöße gegen Datenschutzregelungen nach § 15 des Entwurfs sanktionieren zu können.

3.2 Zur BT-Drucksache 17/4145

3.2.1 Zu Ziffer 2

Die Forderung des Bundesrats nach einer Ende-zu-Ende-Verschlüsselung wird unterstützt (s.o.).

3.2.2 Zu Ziffer 3

Um einen wirklichen Wettbewerb zu erreichen, ist eine einfache Portierbarkeit der De-Mail-Adressen erforderlich. Daher sollte im Gesetz geregelt sein, dass als einheitliche Kennzeichnung „@de-mail.de" verwendet wird und keine providerspezifischen Ergänzungen vorgenommen werden, so das eine typische personalisierte De-Mail-Adresse folgenden Aufbau hat: „Vorname.Nachname.XXXXX@de-mail.de", wobei XXXX für eine zufällige vier- oder fünfstellige Zahl steht, um Adressen von Personen gleichen Namens unterscheiden zu können. Diese Zufallszahl kann bespielsweise von der Bundesnetzagentur vergeben und verwaltet werden.

3.2.3 Zu Ziffer 4:

Für das Gesetzgebungsvorhaben ist eine Eilbedürftigkeit nicht zu sehen. Vielmehr ist bei einem solch grundlegenden Gesetzgebungsvorhaben eine breite und ausführliche Beteiligung der Öffentlichkeit und insbesondere der Fachöffentlichkeit erforderlich. Eine Verabschiedung im Eilverfahren wird dem Vorhaben nicht gerecht.

3.2.4 Zu Ziffer 5:

Die Begründung des Bundesrates für die Zustimmungsbedürftigkeit ist nachvollziehbar, die Begründung der Bundesregierung für die Ablehnung dagegen nicht.

3.2.5 Zu Ziffer 6:

Die Ablehnung der Ziffer 6 des Beschlusses des Bundesrates aus BR-Drucksache 645/10 (Beschluss) (im folgenden BR-Beschluss) und zur Ablehnung angeführte Begründung ist nicht nachvollziehbar. Im Sinne eines normenklaren Gesetzes ist Annahme der Änderung aus Ziffer 6 des BR-Beschlusses zu empfehlen.

3.2.6 Zu Ziffer 8

Der Begriff „sichere Anmeldung", der in § 4 verwendet wird, wird im Gesetzentwurf leider nicht definiert. Selbstverständlich ist es erforderlich, auch nur bei Nutzung von Benutzernamen und Passwort eine sichere Anmeldung (d.h. über https://) zu ermöglichen. § 4 Abs. 3 lässt vermuten, dass mit „unsicherer Anmeldung" etwas anderes als eine unverschlüsselte Übermittlung von Benutzernamen und Passwort gemeint ist.

3.2.7 Zu Ziffer 9

Aus Verbraucherschutzgründen und um den Wettbewerb zu stärken, ist eine Umsetzung dieser Änderung dringend erforderlich (vgl. o. 3.2.2).

3.2.8 Zu Ziffer 10

Aus § 5 Abs. 10 des Gesetzentwurf geht nicht hervor, dass die 90-Tage-Frist zur Löschung erst ab dem Zeitpunkt er ersten sicheren Anmeldung des Nutzers nach dem Eingang der entsprechenden De-Mail in seinem Postfach zu Laufen beginnt. Von daher ist die in der BT-Druchsache 17/3630 vorgeschlagene Regelung zumindest mißverständlich.

3.2.9 Zu Ziffer 11

Dieser Änderungsvorschlag ist zur Umsetzung des Datenschutzes erforderlich.

3.2.10 Zu Ziffer 12

Diesem Änderungsvorschlag sollte aus Verbraucherschutzgründen umgesetzt werden, um eine bessere Akzeptanz von De-Mail zu erreichen. Ein Verweis auf die Begründung dient nicht der Normenklarheit des Gesetzentwurfs.

3.2.11 Zu Ziffer 13

Dieser Vorschlag dient der Normenklarheit des Gesetzentwurfs.

3.2.12 Zu Ziffer 14

Die vom Bundesrat vorgelegten Änderungen sind zur Wahrung des Datenschutzes erforderlich. Dies gilt insbesondere auch für die vorgeschlagene Bußgeldregelung.

3.2.13 Zu Ziffer 15

Bereits bei der Akkreditierung sollten die Anforderungen des Verbraucherschutzes berücksichtigt werden. Nachträgliche Sanktionsmöglichkeiten sind zwar erforderlich, aber aus Sicht des Verbraucherschutzes nicht ausreichend.

3.2.14 Zu Ziffer 18.

Der Begründung des Bundesrates ist nichts hinzuzufügen.

3.2.15 Zu Ziffer 20

Der Prüfauftrag ist aus Gründen der Technikneutralität von Gesetzestexten zu unterstützen.

3.3 Zum Artikel 1 des Entwurfs eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften (BT-Druchsache 17/3630)

Auf die Darstellung des Änderungsbedarf, der durch die obige Aussagen in der Zusammenfassung und zu den Vorschlägen des Bundesrats und des Änderungsantrag bereits dargelegt wurde, wird im Folgenden teilweise verzichtet.

3.3.1 Allgemein

Es ist für die Normenklarheit des Gesetzes erforderlich, das im Gesetzestext verwendete Begriffe, die nicht aus sich selbst heraus klar, sind in einer Begriffsdefinition erläutert werden. Hierzu gehören insbesondere Begriffe wie Eingang einer De-Mail, sichere und unsichere Anmeldung. Der Verweis auf die Begründung ist hier nicht ausreichend.

3.3.2 Zu § 1

Absatz 3 erfüllt nicht die Anforderung an ein Normenklarheit des Gesetzestextes.

3.3.3 Zu § 4

Der Begriff „Sichere Anmeldung" ist ohne Begriffsdefinition missverständlich (s.o. 3.2.6).

3.3.4 zu § 5

In Absatz 2 sollte klar geregelt sein, dass De-Mail-Provider verpflichtet sind, den De-Mail-Nutzer/inne/n mehrere pseudonyme De-Mail-Adressen zur Verfügung zu stellen.

3.3.5 Zu § 7

Die Eintragung im Verzeichnisdienst muss für die Nutzer/innen ohne jede Einschränkung freiwillig sein (vgl. auch die Regelungen im TKG zur Veröffentlichtung von Einträgen im Telefonbuch und in elektronischen Verzeichnissen).

3.3.6 Zu § 8

Mindestanforderungen an die Datensicherheit bei dem Hoch- und Herunterladen von Dokumenten sowie bei der Aufbewahrung der Dokumente sollten bereits im Gesetzestext festgelegt werden.

3.3.7 Zu § 9

Die Informationspflichten sollten um die Information zu pseudonymen De-Mail-Adressen sowie über die unterschiedlichen Risiken mittels „sicherer Anmeldung" und „unsicherer Anmeldung" ergänzt werden.

3.3.8 Zu § 15

s.o., 3.1.1.5 und 3.2.12

3.3.9 zu § 16

Die Regelungen aus Abs. 1 zur Auskunftserteilung werden in der Praxis zu schwierigen Rechtsauslegungsfragen führen, für die die De-Mail-Diensteanbieter zuständig sein sollen. So ist völlig unklar, wie eine Diensteanbieter feststellen soll, ob ein Auskunftsverlangen nicht rechtsmissbräuchlich ist oder gar nur allein dem Zweck dient, dass Pseudonym aufzudecken. Die Abwägung aus Abs. 1 Ziffer 6 stellt sich in der datenschutzrechtlichen Praxis auch häufig als schwierig dar. Gerade bei Auskünf-

ten von Pseudonymen wären konkretere Zulässigkeitsvoraussetzungen erforderlich. Es sollte zumindest im Bereich der Auskunft zu pseudonymen ein Richtervorbehalt geprüft werden.

Die in Absatz 2 enthaltene Pflicht des Diensteanbieters dem das Auskunftsersuchen betrefenden Nutzer (rechtliches?) Gehör zu geben, ist grundsätzlich zu begrüßen, verdeutlicht aber auch, dass hier die Diensteanbieter die Aufgabe erhalten, zwischen Rechtsgütern des Auskunftsersuchenden und des betroffenen Nutzern abzuwägen. Dies ist eine Aufgabe, die üblicherweise von Gerichten übernommen wird.

Es fehlen im § 16 auch Regelungen, die dem betroffenen Benutzer einen Rechtsweg gegen ungerechtfertigte oder gar missbräuchliche Auskunftsersuchen eröffnen würden.

3.3.10 Zu § 18

Bei den Voraussetzungen für die Akkreditierung sollten die Verbraucherschutzbelange ebenfalls berücksichtigt werden (vgl. o, 3.2.13)

3.3.11 Zu § 22

Um die Berücksichtigung der Daten- und Verbraucherschutzbelange dauerhaft zu gewährleisten, sollten im Ausschuss De-Mail-Standardisierung auch Vertreter/innen von Verbraucher- und Datenschutzorganisationen vertreten sein. Damit die Belange der Nutzer/innen ebenfalls berücksichtigt werden, sollten auch Vertreter/innen der Nutzer/innen in diesem Gremium vertreten sein.

3.3.12 Zu § 23

Verstöße gegen § 15 (Datenschutz) sind ebenso wie Verstöße gegen § 17 Absatz 3 (erneute Akkreditierung nach wesentlichen Veränderungen) zu sanktionieren.

Konstanz, 02.02.2011

Werner Hülsmann
- Diplom Informatiker -
Anerkannter Datenschutz-
sachverständiger