State of the art: De-E-Mail

Ein Überblick über De-Mail

mit speziellem Blick auf die kritischen Aspekte

Lars Brozinski

29.01.2011 lars.brozinski@brozinski.de

I. Inhaltsverzeichnis

II. Abkürzungsverzeichnis

BfIT	Beauftragte der Bundesregierung für Informationstechnik
BMI	Bundesministerium des Inneren
BSI	Bundesamtes für Sicherheit in der Informationstechnik
TAN	Transaktionsnummer

III. Tabellenverzeichnis

1. Einleitung

In der modernen Wirtschaftswelt ist eine schnelle Kommunikation ein überlebenswichtiger Faktor. Wenn es um Börsengeschäfte oder Kaufverträge geht, müssen Management-Entscheidungen schnell gefällt werden. Dies stellt in den wenigsten Fällen ein Problem dar. Das zeitliche Nadelöhr jedoch liegt in dem Kommunikationsweg zum Empfänger. Einen Papierbrief zuzustellen, dauert innerhalb Deutschlands mindestens einen Tag. Ein Fax ist schneller, bietet jedoch im herkömmlichen Ausdruck eher eine mindere Qualität. Schneller, lesbarer und leichter weiter zu verarbeiten ist nur die seit 1984[1] in Deutschland vorhandene E-Mail. Innerhalb weniger Sekunden oder Minuten ist eine E-Mail beim Empfänger angekommen. Doch wie ist es mit der Rechtsgültigkeit einer E-Mail? Eine E-Mail entspricht der Schriftform nach §126a BGB. Ihr fehlt somit die erforderliche Originalunterschrift[2], welche beim Postbrief gegeben ist. Beim herkömmlichen Brief sowie bei der E-Mail handelt es sich, wenn ein Kaufvertrag geschlossen werden soll, um eine Willenserklärung unter Abwesenden gemäß §130 BGB. Diese wird in dem Zeitpunkt wirksam, in welchem sie in den Machtbereich des Empfängers gelangt, und er die Möglichkeit hatte sie nach üblichen Verhältnissen zur Kenntnis zu nehmen.[3]

Ein Brief ist somit zugegangen, wenn er im Briefkasten des Empfängers eingeworfen wurde. Wird er abends eingeworfen, ist er erst am nächsten Morgen zur gewöhnlichen Zustellungszeit zugegangen. Eine E-Mail ist dann zugegangen, wenn sie sich auf dem E-Mail-Server des Empfängers, also in dessen Machtbereich, befindet. Trifft sie dort spät abends ein, so ist, auch bei Privatpersonen, der Zugang nach herrschender Meinung erst am nächsten Tag anzunehmen[4]. Wichtig wird der Zeitpunkt des Zugangs, wenn es um Vertragsannahme oder -rücktritt, Gewährleistungen und Garantien geht. Unter Umständen kann die eine Stunde, die ein Brief zu spät im Briefkasten gelandet ist, einen Kaufvertrag nichtig werden lassen. Ebenso ist die Fälschungssicherheit, gerade bei E-Mails, eher gering. Mit De-Mail versucht die Bundesregierung ein Instrument zu etablieren, das eindeutiger und sicherer ist als die bisherigen Kommunikationsmittel.

---

[1] Vgl. Oversohl /25 Jahre E-Mail/ o. S.

[2] Vgl. Weyand /Handels- und Gesellschaftsrecht/ S. 20

[3] Vgl. Weyand /Bürgerliches Recht/ S. 71-72

[4] Vgl. Leipold /BGB I/ S.159

Die vorliegende Arbeit wird einen groben Überblick über die De-Mail geben und aufzeigen, wo es Schwächen und Probleme gibt.

Die Ausarbeitung erfolgt als verbalsprachliche Analyse der Primärliteratur zum Thema De-Mail. Als Quellen für den Überblick werden die offiziellen Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik[5], des Bundesministeriums des Inneren[6] und der Beauftragten der Bundesregierung für Informationstechnik[7] genutzt. Um die Nachteile und kritischen Meinungen abzubilden, werden relevante Fachjournalveröffentlichungen herangezogen, da derzeit keine Bücher die Situation adäquat wiedergeben. Ziel ist es, die nachteiligen Kernpunkte herauszuarbeiten und so neutral wie möglich zu beschreiben.

Zuerst werden in sachlogischer Reihenfolge die Schritte abgearbeitet, die ein neuer Nutzer durchführen muss um De-Mail zu verwenden. Hierbei werden kurz die Anbieter und deren Angebote verglichen sowie die Registrierung und Validierung beschrieben. Danach werden Versandoptionen und ihre rechtlichen Bedeutungen betrachtet. Es folgen die grundlegenden Sicherheitsmerkmale sowie der Datensafe und der Identitätsbestätigungsdienst.

Wann immer es angebracht ist, werden die Nachteile und die Kritik ergänzend dargestellt. Zum Schluss erfolgt ein Ausblick auf die zukünftige Entwicklung der De-Mail und eine kritische Reflektion des Inhalts dieser Arbeit.

2. Anmeldung

2.1 Anbieter

Aktuell gibt es in Deutschland sechs De-Mail-Anbieter: Die Deutsche Telekom, T-Systems, GMX, WEB.DE (United Internet AG) sowie Signaturportal.de und Govmail.de, (Mentana-Claimsoft AG) sind. Die Deutsche Telekom widmet sich ausschließlich den Privatkunden[8], T-Systems hingegen den Unternehmen[9]. Govmail.de

[5] Im Folgenden nur noch „BSI“ genannt

[6] Im Folgenden nur noch „BMI“ genannt

[7] Im Folgenden nur noch „BfIT“ genannt

[8] Vgl. Deutsche Telekom /Telekom pusht De-Mail/ o. S.

[9] Vgl. T-Systems /Rechtsverbindlich De-Mailen/ o. S.

versteht sich als Ansprechpartner für die Verwaltung[10]. GMX, WEB.DE und Signaturportal.de geben keine konkrete Zielgruppe an. Grundvoraussetzung für die Nutzung bei den etablierten E-Mail Diensten GMX, WEB.DE und der Telekom ist ein bestehendes E-Mail-Konto bei dem Anbieter.[11] Bei den restlichen Anbietern gibt es keine genaueren Informationen. Die Registrierung und das Empfangen von De-Mails ist, soweit die Anbieter es erwähnen, entgeltfrei.[12] Wie hoch die Versandkosten sind, wird laut den Anbietern noch verhandelt, sie sollen jedoch günstiger sein als das Porto eines Standardbriefs und eines E-Postbriefs der deutschen Post.[13] WEB.DE gibt an, dass derzeit 15 Cent zur Debatte stehen.[14] Darüber hinaus bietet die Telekom eine nicht näher bezifferte Anzahl von Gratis-De-Mails an.[15]

2.2 Akkreditierung

Grundlage für De-Mail wird das De-Mail-Gesetz (ehemals „Bürgerportalgesetz“[16]) sein, welches aktuell im Entwurf vom 13. Oktober 2010 vorliegt.[17] Um als offizieller De-Mail-Anbieter zu gelten, muss ein Unternehmen eine Akkreditierung durch das BSI bzw. eine vom BSI lizensierte Prüfstelle[18] vornehmen lassen.[19] Ist diese erfolgreich, erhält der Portalbetreiber ein Gütesiegel und darf die Second-Level-Domain „De-Mail“ benutzen.[20] Voraussetzung für eine erfolgreiche Akkreditierung ist, dass der Betreiber über die notwendige technische, organisatorische und rechtliche Fachkunde verfügt.[21]

[10] Vgl. Govmail.de /Startseite/ o. S.

[11] Vgl. Deutsche Telekom /Telekom pusht De-Mail/; GMX /Einfach wie E-Mail/; WEB.DE /Häufige Fragen/ jeweils o. S.

[12] Vgl. Deutsche Telekom /Telekom pusht De-Mail/; GMX /Häufige Fragen/; WEB.DE /Häufige Fragen/; Signaturportal.de /Elektronische Rechnung/ jeweils o. S.

[13] Vgl. GMX /Häufige Fragen/; WEB.DE /Häufige Fragen/ jeweils o. S.

[14] Vgl. WEB.DE /Häufige Fragen/ o. S.

[15] Vgl. Deutsche Telekom /Telekom pusht De-Mail/ o. S.

[16] Vgl. BSI /Infrastruktur/ o. S.

[17] Siehe BMI /Gesetz/

[18] Vgl. Schumacher /Akkreditierung/ S.304

[19] Vgl. BMI /Technische Details/ o. S.

[20] Vgl. Roßnagel u. a. /De-Mail und Bürgerportale/ S. 732

[21] Vgl. Schumacher /Akkreditierung/ S. 303

Er muss in der Lage sein das System mit den anderen Anbietern zusammenzuschließen, genügend finanzielle Mittel haben, um mögliche Schadensersatzzahlungen aufgrund von fehlerhaftem Angebot aufzubringen, das De-Mail Angebot nach der technischen Richtlinie des BSI umsetzen und die datenschutzrechtlichen Anforderungen erfüllen.[22] Die Technische Richtlinie des BSI wird mindestens einmal pro Jahr auf ihre Aktualität geprüft und bei Bedarf angepasst. Weiterhin muss der De-Mail-Anbieter sich jedes Jahr einer Prüfung unterziehen und alle drei Jahre die komplette Akkreditierung erneut durchlaufen.[23]

2.3 Kritik: Organisation

Die De-Mail Infrastruktur soll durch technische Komponenten und organisatorische Maßnahmen, wie etwa Arbeitsteilung und dem Vier-Augen-Prinzip[24], vor Zugriffen der Mitarbeiter gesichert werden.[25] Kritisch anzumerken ist, dass ein physischer Zugriff auf eine IT-Struktur immer mit großem Risiko verbunden ist. Ein Beispiel dafür ist der Diebstahl brisanter Daten im Fall der Steuersünder-CD[26] Anfang des Jahres 2010.
Es kann sich erst im praktischen Arbeitsalltag zeigen, wie gut die organisatorischen Maßnahmen zum Schutz wirklich sind.

2.4 Kritik: Anbieterwechsel

Will der Nutzer den De-Mail-Anbieter wechseln, so wird sein Konto gelöscht und die De-Mail Adresse wieder freigegeben. Er hat keine Garantie, seine bisherige Adresse, wie bspw. eine Telefonnummer, zu dem neuen Anbieter mitnehmen zu können.[27] Dadurch entsteht für den Nutzer eine Marktaustrittsbarriere. Ein manueller Transfer der Daten wird ebenfalls erschwert, da der Export von Nachrichten und Inhalten zwar standardmäßig vorgesehen ist, jedoch der Import eben solcher nur optional angeboten werden muss.[28]

---

[22] Vgl. Roßnagel u. a. /De-Mail und Bürgerportale/ S. 732

[23] Vgl. BSI /Sicherheitsfunktionen/ S. 11

[24] Vgl. Röhm, Fuchs /System-Entwicklung/ S. 543

[25] Vgl. BSI /Sicherheitsfunktionen/ S. 4

[26] Vgl. Spiegel Online /Steuerbetrüger-CD/ o. S.

[27] Vgl. Lapp /Brauchen wir De-Mail/ S. 654

[28] Vgl. BSI /Technische Richtlinie/ S. 96

2.5 Registrierung und Validierung

Damit die Nutzer von De-Mail sich auf die eindeutige Identifikation ihres Gegenübers verlassen können, werden bei der Registrierung einer De-Mail Adresse nur Verfahren mit hohem Sicherheitsstandard zugelassen.[29] Darunter fällt bspw. die Identifikation mittels des elektronischen Personalausweises oder des Post-Ident-Verfahrens. Natürliche Personen müssen bei der Registrierung Pflichtdaten wie Vor- und Nachname, Geburtsdatum und Meldeadresse angeben. Juristische Personen müssen neben den Angaben zu ihrer Person auch die Daten ihrer natürlichen Vertreter angeben. Eine De-Mail Adresse sieht wie folgt aus: <Vorname>.<Nachname>@<De-Mail-Anbieter>.de-mail.de.[30] Gibt es schon eine registrierte Adresse mit dem Namen einer Person, wird die De-Mail-Adresse um eine Zahl ergänzt.[31] Neben der regulären Adresse können auch weitere pseudonyme De-Mail Adressen angelegt werden. Diese haben die Form: pn_<Pseudonym>@<De-Mail-Anbieter>.de-mail.de. Eine juristische Person hat darüber hinaus die Möglichkeit sich einen ganzen Adressraum zu registrieren und den lokalen Teil, also die Bezeichnung vor dem @-Zeichen, selbst zu bestimmen. Formal sieht eine solche De-Mail Adresse wie folgt aus: <Bezeichnung>@<Firma>.de-mail.de. Die juristische Person kann eine Vielzahl von lokalen Adressen erstellen, bspw. eine für jede Abteilung.

Dem Nutzer steht es frei sich in den Verzeichnisdienst von De-Mail einzutragen, um dort neben seinen persönlichen Daten auch öffentliche Schlüssel[32] zu hinterlegen.[33]

2.6 Kritik: Pseudonym

Die Pseudonym Adresse ist in erster Linie für Personen mit Künstlernamen attraktikv. Ein herkömmlicher Nutzer könnte ein Pseudonym jedoch mit Anonymität verwechseln. In seinen Augen sollte für den Empfänger keine Rückschlussmöglichkeit auf den Sender möglich sein. Die Pseudonym Adresse ist jedoch im System des De-Mail-Anbieters mit der real existierenden Person verknüpft. Der Nutzer möchte anonym sein, dennoch ist es möglich durch das Zusammenführen verschiedener Datensätze

[29] Vgl. BMI /Technische Details/ S. 2

[30] Vgl. Absatz mit: BMI /Technische Details/ S. 2

[31] Vgl. WEB.DE /Häufige Fragen/ o. S.

[32] Siehe dazu Kapitel 3.1.3 Signatur und Verschlüsselung

[33] Vgl. BfIT /Verzeichnisdienst/

Bewegungsprofile zu erstellen. Weiterhin ist es denkbar, dass im Zuge der Strafverfolgung oder Gefahrenabwehr der De-Mail-Anbieter dazu gezwungen werden kann die Daten des Nutzers offenzulegen.[34]

3. Angebotene Dienste

3.1 De-Mail

3.1.1 Anmeldung

Für eine Anmeldung bei einem De-Mail Konto steht im einfachsten Fall eine Weboberfläche zur Verfügung. Es ist aber auch möglich seine Nachrichten mittels eines E-Mail Clienten abzurufen.[35]

Es gibt zwei Authentisierungsniveaus mittels derer sich ein Nutzer am De-Mail-System anmelden kann.[36] Normal bedeutet Anmeldung durch Benutzername und Passwort – sprich Wissen. Das Anmeldeniveau „Hoch“ erfordert Besitz und Wissen, wobei Besitz einen identifizierenden Gegenstand meint[37].

Dafür in Frage kommen Chipkarten wie der elektronische Personalausweis oder Signaturkarten, Spezielle USB-Geräte (Dongle), auf Mobiltelefone übermittelte TAN oder Einmalpasswörter.[38] Für verschiedene Aktionen innerhalb des De-Mail-Systems benötigt man entweder Normal oder „Hoch“ als Authentisierungsniveau.[39]

Sollte ein Nutzer sein Passwort oder seinen Token verlieren, kann er sein Konto über eine Hotline sperren lassen.[40] Ihm wird dann ein neues Passwort oder ein Token zugesendet. Hat er neben dem verlorenen Token einen weiteren, so kann er sich damit weiterhin anmelden. Nur der verlorene Token wird gesperrt.

---

[34] Vgl. Schulz /Rechtsprobleme/ S. 602

[35] Vgl. BMI /Technische Details/ S. 4

[36] Vgl. Absatz mit BMI /Technische Details/ S. 3

[37] Im Folgenden nur noch “Token” genannt

[38] Vgl. BfIT /Token/ o. S.

[39] Siehe dazu Kapitel 3.1.2 Versandoptionen und -arten

[40] Vgl. Absatz mit: BfIT /Passwort vergessen/ o. S.

3.1.2 Versandoptionen und -arten

Es gibt fünf Versandoptionen, die der Nutzer beim Senden einer De-Mail wählen kann.[41] Wenn keine weitere Angabe zum Authentisierungsniveau gemacht wird, reicht eine Normal-Anmeldung aus. Die Option „Persönlich“ zwingt den Empfänger dazu sich mit dem Authentisierungsniveau „Hoch“ anzumelden, um die Nachricht lesen zu können. Der Sender muss für den Versand ebenfalls mit „Hoch“ eingeloggt sein. Mit der Option „Absenderbestätigt“ wird dem Empfänger mitgeteilt, dass der Sender mit dem Authentisierungsniveau „Hoch“ angemeldet war und somit zum Ausdruck bringt, dass die Nachricht für ihn verbindlich ist. Wird die Option „Versandbestätigt“ gewählt, erhält der Sender von seinem eigenen De-Mail-Anbieter eine Versandbestätigung. Die Option „Eingangsbestätigung“ schickt sowohl eine Nachricht an den Sender, als auch an den Empfänger, sobald die Nachricht beim De-Mail-Anbieter des Empfängers eingegangen ist. Bei der Versandoption „Abholbestätigt“ wird eine Nachricht vom De-Mail-Anbieter des Empfängers an Sender und Empfänger geschickt, wenn der Empfänger sich mit dem Authentisierungsniveau „Hoch“ angemeldet hat.

De-Mail bietet drei verschiedene vordefinierte Versandarten, die versuchen Nachbildungen von physischen Postbrief-Versandarten zu sein.[42] Eine Nachricht die mit der Versandart „De-Mail“ versendet wird hat keine Versandoptionen. Sie wird aber durch die standardmäßigen Sicherheitsmaßnahmen gegen das Mitlesen unberechtigter Dritter geschützt. Wird die Versandart „De-Mail-Einschreiben“ gewählt, sind die Versandoptionen „Versandbestätigung“ und „Eingangsbestätigung“ gewählt. Der Sender erhält somit eine Bestätigung, wann er die Nachricht verschickt hat und wann sie im Postfach des Empfängers eingetroffen ist. Die Versandart „De-Mail Förmliche Zustellung“ aktiviert die Versandoptionen „Persönlich“, „Versandbestätigung“, „Eingangsbestätigung“ und „Abholbestätigung“. Der Sender erhält eine Bestätigung, wann er die Nachricht versendet hat, wann sie im Postfach des Empfängers eingetroffen ist und wann der Empfänger sich nach dem Eintreffen mit dem Authentisierungsniveau „Hoch“ angemeldet hat.

Zur übersichtlicheren Darstellung des Kapitels dient die Tabelle 1, in welcher den Versandarten die zugehörigen Versandoptionen zugeordnet sind.

---

[41] Vgl. Absatz mit: BSI /Technische Richtlinie/ S.17-20

[42] Vgl. Absatz mit: BSI /Technische Richtlinie/ S. 18

	Versandoptionen				
Versandarten von De-Mail	Persönlich	Absenderbestätigt	Versandbestätigung	Eingangsbestätigung	Abholbestätigung
De-Mail					
De-Mail Einschreiben			X	X	
De-Mail Förmliche Zustellung	X		X	X	X

Tabelle 1: Versandarten und die dazugehörigen Versandoptionen[43]

3.1.3 Kritik: Authentifizierung und Versandoptionen

Das De-Mail-Gesetz verlangt von den De-Mail-Anbietern, dass mindestens zwei Anmeldeverfahren, nämlich Normal und „Hoch“, für den Nutzer zur Auswahl bereit stehen. Die Kombination aus Benutzername und Passwort beim Niveau „Normal“ ist als alleiniger Sicherungsmechanismus jedoch nicht sicher genug, weil er durch Phishing-Angriffe[44] oder Social Engineering[45] leicht zu überwinden ist.

Wenn nur die Anmeldung mit dem Authentifizierungsniveau „Hoch“ möglich sein würde, befürchtet der Gesetzgeber die Gefahr eines Akzeptanzproblems beim Nutzer.[46] Der Nutzer stünde bei jeder Nachricht vor dem Problem der Komplexität der Versandoptionenwahl. Eine De-Mail, die aber nur Normal authentifiziert ist, gilt bei den Gerichten bislang als nicht ausreichend zur Feststellung der Identität.

Ebenso wird die teilweise durch Gesetz vorgeschriebene Schriftform durch eine De-Mail nicht erfüllt.[47] Bspw. benötigt ein Widerspruch gegen einen behördlichen Verwaltungsakt die Schriftform.[48] Jedoch kann diese durch die elektronische Form

[43] Korrigierte Tabelle vgl. BSI /Technische Richtlinie/ S. 19

[44] Vgl. Laudon u.a. /Wirtschaftsinformatik/ S. 1011

[45] Vgl. Lipski /Social Engineering/ S. 7

[46] Vgl. Absatz mit: Lapp /Brauchen wir De-Mail/ S. 653-654

[47] Vgl. BfIT /Rechtsgeschäfte/ o. S.

[48] Vgl. Bundesministerium der Justiz /VwGO/ o. S.

ersetzt werden, wenn eine qualifizierte elektronische Signatur benutzt wird.[49] Eine qualifizierte elektronische Signatur ist aber nicht standardmäßig Bestandteil von De-Mail, sondern nur in Verbindung mit dem Authentisierungsniveau „Hoch“ oder externen Signaturkomponenten.[50] Die rechtlichen Vorteile wären also schon vorhanden, wenn der Nutzer lediglich eine E-Mail mit einer qualifizierten elektronischen Signatur benutzen würde.[51] Die angepriesene Rechtssicherheit von De-Mail ist somit in Fällen, die eine Schriftform oder elektronische Form benötigen, nicht gewährt. Dieser Sachverhalt mündet direkt in die Wettbewerbswidrigkeit. Laut dem §5 Abs. 1 UWG handelt ein Unternehmen wettbewerbswidrig, wenn es über wesentliche Merkmale einer Ware oder Dienstleistung, wie bspw. Vorteile, Risiken etc., unwahre oder sonstige zur Täuschung geeigneten Angaben macht.[52] Das BMI wirbt in seiner Informationsbroschüre mit „De-Mail wird das rechtsverbindliche und vertrauliche Versenden von Dokumenten und Nachrichten über das Internet ermöglichen“.[53] Hier wird ein Eindruck von Rechtssicherheit erzeugt der aber, wenn überhaupt, nur mit dem Authentifizierungsniveau „Hoch“ erreicht werden kann. Die De-Mail-Anbieter laufen somit Gefahr einer Beschwerdewelle wegen falscher Versprechungen gegenüberzustehen.

3.1.4 Kritik: Zustellungszeitpunkt

Im Zuge der Neuregelung des Verwaltungszustellungsgesetzes genügt zum Nachweis der elektronischen Zustellung die elektronische Zugangsbestätigung.[54] De-Mail benutzt in der Zugangsbestätigung Datum und Uhrzeit des Eingangs der Nachricht im Postfach. Bisher gilt bei Briefpost der Zugang eines Einschreibens ab dem Zeitpunkt der Übergabe durch den Postzusteller oder am dritten Tag nach der Postaufgabe. Wenn der Empfänger einen späteren Zugang nachweisen kann, gilt dieser Tag. Im Zweifel allerdings muss die Behörde den Zugangszeitpunkt nachweisen. Durch die Neuregelung entsteht eine Verschiebung der Verwaltungsverfahrensregeln zu Lasten des De-Mail-

[49] Vgl. Bundesministerium der Justiz /VwVfG/ o. S.

[50] Vgl. BSI /Infrastruktur/ o. S.

[51] Vgl. Lapp /Brauchen wir De-Mail/ S. 652

[52] Vgl. Bundesministerium der Justiz /UWG/ o. S.

[53] BMI /De-Mail Informationsbroschüre/ S. 3

[54] Vgl. Absatz mit: Lapp /Brauchen wir De-Mail/ S. 652-653

Nutzers. Er muss sich selbstständig, ohne Rücksicht auf Urlaubs- oder Krankheitszeiten, um die Kenntnisnahme seiner De-Mails kümmern. Unterlässt er dies, beginnt die Frist bereits ohne sein Wissen zu laufen, wodurch sich bspw. Widerspruchsfristen verkürzen.

3.1.5 Signatur und Verschlüsselung

Eine normale E-Mail wird ohne spezielle Einstellungen nie verschlüsselt versendet und ist dadurch im Klartext lesbar.[55] Des Weiteren enthält eine E-Mail keinen Identitätsbeweis. De-Mail hingegen ist so konzipiert, dass der Nutzer keine zusätzliche Software auf seinem Computer installieren muss, um ein hohes Maß an Sicherheit zu erhalten. Eine De-Mail wird grundsätzlich verschlüsselt versandt.[56] Zuerst erstellt der eigene De-Mail-Anbieter zur Sicherung der Integrität eine Prüfsumme der Nachricht.[57] Dadurch ist prüfbar ob eine Manipulation an den Daten vorgenommen wurde.[58] Wird die Nachricht mit der Versandoption „Absenderbestätigt“[59], „Versandbestätigt“[60], „Eingangsbestätigt“[61] oder „Abholbestätigt“[62] verschickt, erhält sie vom De-Mail-Anbieter zusätzlich eine qualifizierte elektronische Signatur.[63] Dann wird eine Punkt-zu-Punkt-Verschlüsselung, also ein Tunnel, zwischen dem De-Mail-Anbieter des Senders und des Empfängers aufgebaut, mittels dessen die Nachricht übertragen wird. Ein Transport der De-Mail als normale E-Mail in das Internet, sowie der umgekehrte Fall, ist nicht möglich.[64] Bevor die Nachricht im Postfach des Empfängers auftaucht, wird sie noch vom De-Mail Anbieter auf Viren und Trojaner überprüft[65], sowie

[55] Vgl. Halb /Verschlüsselung/ S. 16

[56] Vgl. BfIT /Sicherheit/ o. S.

[57] Vgl. BMI /Technische Details/ o. S.

[58] Vgl. BSI /Sicherheitsfunktionen/ S. 5

[59] Vgl. BSI /Technische Richtlinie/ S. 55

[60] Vgl. BSI /Technische Richtlinie/ S. 58

[61] Vgl. BSI /Technische Richtlinie/ S. 73

[62] Vgl. BSI /Technische Richtlinie/ S. 68

[63] Vgl. BSI /Sicherheitsfunktionen/ S. 5

[64] Vgl. BSI /Sicherheitsfunktionen/ S. 4

[65] Vgl. BSI /Infrastruktur/ o. S.

verschlüsselt gespeichert[66]. Die De-Mail muss spätestens nach acht Stunden im Postfach des Empfängers liegen.[67]

Neben diesem Standardvorgang haben die Nutzer noch die Möglichkeit die Nachricht selbst Ende-zu-Ende zu verschlüsseln.[68] Der Sender verschlüsselt seine Nachricht auf seinem eignen Computer und sendet sie per De-Mail zum Empfänger, welcher sie seinerseits auf seinem Computer wieder entschlüsselt. Für diese höhere Sicherheit ist eine zusätzliche Software, sowie ein privater und ein öffentlicher Schlüssel notwendig. Der Verzeichnisdienst des De-Mail-Anbieters bietet die Möglichkeit den öffentlichen Schlüssel zu tauschen.

Für Behörden und Unternehmen bieten sich noch vielfältige Möglichkeiten De-Mail an ihre bereits vorhandene Infrastruktur anzupassen.[69] So können bspw. interne E-Mails über ein Gateway zu De-Mails umgewandelt werden.

3.1.6 Kritik: Verschlüsselung

Zur Sicherung der Vertraulichkeit, Integrität und Authentizität wird von den De-Mail-Anbietern regulär nur eine Verbindungsverschlüsselung angeboten, die aber nicht verhindert, dass Mitarbeiter innerhalb des De-Mail-Netzwerkes die Nachricht im Klartext lesen können. Diese Problematik der Organisation der De-Mail-Anbieter wurde schon im Kapitel 2.2.1 aufgegriffen. Die Konferenz der Datenschutzbeauftragten schlägt zur Abmilderung dieses Risikos vor, die optionale Ende-zu-Ende-Verschlüsselung verpflichtend zu machen.[70]

3.2 De-Safe

Die De-Mail-Anbieter stellen eine verschlüsselte und integritätsgeschützte[71] Dokumentenablage bereit, die als langzeitiger Aufbewahrungsort für wichtige elektronische Unterlagen wie Verträge, Verwaltungsbescheide oder De-Mails genutzt werden kann. Die in De-Safe abgelegten Daten können mit einer Suchfunktion

[66] Vgl. BSI /Sicherheitsfunktionen/ S. 5

[67] Vgl. BSI /Technische Richtlinie/ S. 22

[68] Vgl. Absatz mit: BSI /Infrastruktur/ o. S.

[69] Vgl. Absatz mit: BMI /Anbindung juristischer Personen/ S. 14

[70] Vgl. o. V. /Konferenz Datenschutzbeauftragte/ S. 424

[71] Vgl. BMI /Technische Details/ S. 3

gefunden werden.[72] Für den Zugriff auf De-Safe ist das Authentisierungsniveau „Hoch“ erforderlich.[73]

3.3 Kritik: De-Safe

Die mit De-Safe angebotene sichere Verwaltung von Daten wird heute schon von vielen Anbietern im Internet angeboten.[74] Es gibt zurzeit keinen Zusatznutzen der De-Safe als notwendige technische Neuerung für eine vertrauenswürdige und rechtssichere Kommunikation rechtfertigt.

Zukünftig könnten weitere Funktionen De-Safe aufwerten um dem Grundgedanken von De-Mail gerecht zu werden. Zu nennen wäre die Möglichkeit bereits signierte Dokumente mit einer weiteren Signatur des De-Mail-Systems zu versehen oder elektronische Dokumente Dritten zum Abruf zur Verfügung zu stellen.[75]

3.4 De-Ident

Der De-Mail-Anbieter kann einen Identitätsbestätigungsdienst anbieten, der es dem Nutzer erlaubt sich gegenüber einem Dritten schnell und sicher auszuweisen.[76] Der Nutzer will bspw. einen Onlinekauf abschließen und muss dafür sein Alter bestätigen. Dazu muss er mit dem Authentisierungsniveau „Hoch“ angemeldet sein[77] und der De-Mail-Adresse des Onlineshops eine Ident-Karte zusenden, in der die gewünschten Angaben enthalten sind. Der De-Mail-Anbieter muss mindestens die in Tabelle 2 dargestellten Ident-Karten mit den entsprechenden Attributen anbieten.

[72] Vgl. Gelzhäuser /Pilotprojekt/ S. 647

[73] Vgl. BSI /Technische Richtlinie/ S. 92

[74] Vgl. Absatz mit: Schulz /Rechtsprobleme/ S. 602

[75] Vgl. Roßnagel u. a. /De-Mail und Bürgerportale/ S. 731

[76] Vgl. BMI /Gesetz/ S. 6

[77] Vgl. BSI /Technische Richtlinie Identifizierungsdienst/ S. 7

Identitätskarte einer natürlichen Person	Adress-Karte einer natürlichen Person	Alters-Karte einer natürlichen Person	Identitätskarte einer Institution	De-Mail-Adress-Karte
Name Vorname Straße* Hausnummer* Ort* Staat* Geburtsdatum Geburtsort **Hauptwohnsitz*	Name Vorname Straße* Hausnummer* Ort* Staat*	Altersangabe in Jahren Alterskategorie 16 Jahre oder älter Alterskategorie 18 Jahre oder älter	Langform des Namens Straße Hausnummer Ort Staat Geschäftsfeld/Gegenstand der Organisation Vertretungsberechtigte Person Name Vorname	De-Mail-Adresse

Tabelle 2: Ident-Karten[78]

Die Identifizierungs-De-Mail wird mit der Versandoption „Persönlich“[79] sowie dem Datum und der Uhrzeit der letzten Änderung eines Identitätsattributs[80] ausgestattet und anschließend qualifiziert elektronisch signiert.[81] Eine Kopie wird an den Nutzer gesendet, um nachvollziehen zu können welche Ident-Bestätigungen er bereits getätigt hat.[82] Eine Ident-Bestätigung muss spätestens innerhalb einer Minute beim Empfänger, und als Kopie beim Sender, eintreffen.[83] Der Empfänger prüft die Ident-Bestätigung und muss diese dann selbstständig einem Geschäftsvorfall zuordnen, da das Auftragssystem außerhalb des Einflussbereiches von De-Mail steht.[84]

3.5 Kritik: De-Ident

Das BSI behauptet zwar, es gäbe eine Pflicht für den Kontoinhaber seine Identitätsdaten, z. B. den Vertreter einer juristischen Person oder die Adresse, zu

[78] Vgl. BSI /Technische Richtlinie Identifizierungsdienst/ S. 8-9

[79] Vgl. BSI /Technische Richtlinie Identifizierungsdienst/ S. 11

[80] Vgl. BSI /Technische Richtlinie Identifizierungsdienst/ S. 8

[81] Vgl. BSI /Technische Richtlinie Identifizierungsdienst/ S. 10

[82] Vgl. BSI /Technische Richtlinie Identifizierungsdienst/ S. 11

[83] Vgl. BSI /Technische Richtlinie Identifizierungsdienst/ S. 14

[84] Vgl. BSI /Technische Richtlinie Identifizierungsdienst/ S. 12

aktualisieren[85], aber im De-Mail-Gesetz findet sich keine Grundlage um dies zu belegen.[86] Die Behörde kann nur dann die Sperrung eines Identitätsdatums anordnen, wenn die Annahme besteht, dass es aufgrund falscher Tatsachen ausgestellt wurde oder nicht ausreichend fälschungssicher ist. Wie genau im Falle des Erlöschens einer juristischen Person, sowie dem Tod oder der Geschäftsunfähigkeit einer natürlichen Person zu verfahren ist, wird im De-Mail-Gesetz nicht geregelt. Der Empfänger einer Ident-Bestätigung kann sich also nicht darauf verlassen, korrekte Informationen zu bekommen. Lediglich der mitgesendete Zeitstempel der Identifikationsdaten kann ihn vermuten lassen, dass es sich um historische Daten handelt.

4. Schlussbemerkung

De-Mail wird wahrscheinlich im März 2011 offiziell starten.[87] Die überwiegende Zahl der Berichterstattungen sieht De-Mail positiv. 90% der Testnutzer des Pilotprojekts in Friedrichshafen würden De-Mail weiterempfehlen und 60% der deutschen Internetnutzer gaben an De-Mail nutzen zu wollen.[88] Die am Pilotprojekt beteiligten Unternehmen sehen viele Vorteile in De-Mail. Der Gesamtverband der Deutschen Versicherungswirtschaft e. V. z. B. sieht durch De-Mail Einsparungspotenzial von mehreren 100 Millionen Euro pro Jahr.[89] Es ist denkbar, dass es für viele Institutionen reizvoll erscheint durch De-Mail Kosten für Papier, Porto, Druck, Umschläge und auch Zeit einzusparen.

Anfangs werden vor allem Behörden, mittlere und große Unternehmen sowie Freiberufler De-Mail nutzen.[90] Für viele Privatpersonen werden die Vorteile der elektronischen Zustellung mit zunehmender Verbreitung sichtbar werden. Hier wären Abruf und Versand der Nachrichten von überall, Verarbeitung und platzsparende Archivierung von Dokumenten und geringerer Zeitaufwand für Behördenkommunikation zu nennen.

---

[85] Vgl. BSI /Sicherheitsfunktionen/ S. 7

[86] Vgl. Absatz mit: Lapp /Brauchen wir De-Mail/ S. 654

[87] Vgl. Haufe /Nachbesserung/ o. S.

[88] Vgl. Gelzhäuser /Pilotprojekt/ S. 647

[89] Vgl. BMI /De-Mail Informationsbroschüre/ S. 14

[90] Vgl. Absatz mit: Roßnagel u. a. /De-Mail und Bürgerportale/ S. 734

Ähnliche Vorteile gab es auch bei der Einführung des Online-Bankings. Im Jahr 2008 nutzten bereits 35% der Deutschen Online-Banking.[91] Beim Online-Banking wird wie bei De-Mail ein Token als Authentifizierungssystem verwendet. Der Komplexitätsgrad ist also ähnlich. Zieht man daraus eine Analogie, scheint ein Erfolg von De-Mail vorstellbar.

Bisher gab es nur eine geringe Anzahl kritischer Berichterstattungen, von denen einige Probleme ansprachen, die in jüngster Zeit bereits gelöst wurden. Neben der unklaren Rechtssicherheit ist der Preis der kritischste Punkt. Werden die Kosten eher dem Bürger als den Institutionen aufgezwungen kann dies die Akzeptanz beeinträchtigen.[92] Die besprochenen kritischen Sicherheitsmerkmale und rechtlichen Unklarheiten werden wahrscheinlich im Zuge der kontinuierlichen Weiterentwicklung von De-Mail[93] schnell überarbeitet werden, so dass die Kritik immer leiser wird.

Mit dieser Arbeit sind die wesentlichen Merkmale von De-Mail in einem angemessenen Umfang gebündelt worden. Da es bisher nur Meinungen von Juristen, aber keine Urteile gibt, konnte nur sehr grob und oberflächlich auf die rechtlichen Probleme eingegangen werden. Weiterhin wurde die Thematik des De-Mail-Gateway nur kurz angeschnitten. Dort gibt es noch viele beachtenswerte Kritikpunkte, die zukünftig untersucht werden könnten. Das größte Problem stellte die Überprüfung der Kritik auf ihre Aktualität hin dar. Oft wurden die kritischen Meinungen von Verantwortlichen gehört und der Entwurf des De-Mail-Gesetzes daraufhin angepasst.

[91] Vgl. Bitkom /Online-Banking/ o. S.

[92] Vgl. Roßnagel u. a. /De-Mail und Bürgerportale/ S. 734

[93] Vgl. BSI /Sicherheitsfunktionen/ S. 11

5. Literaturverzeichnis

BfIT /Passwort vergessen/

Die Beauftragte der Bundesregierung für Informationstechnik: Was passiert, wenn man sein Passwort vergessen den Token verloren hat?, http://www.cio.bund.de/cln_164/SharedDocs/FAQs/DE/F/F51.html?nn=586022, Berlin 2010, Abruf: 2010-11-20

BfIT /Rechtsgeschäfte/

Die Beauftragte der Bundesregierung für Informationstechnik: Kann man mit De-Mail Rechtsgeschäfte abschließen?, http://www.cio.bund.de/cln_164/SharedDocs/FAQs/DE/C/C29.html?nn=586022, Berlin 2010, Abruf: 2010-11-20

BfIT /Sicherheit/

Die Beauftragte der Bundesregierung für Informationstechnik: Sicherheit, http://www.cio.bund.de/cln_164/DE/IT-Projekte/De-Mail/Sicherheit/sicherheit_node.html, Berlin 2010, Abruf: 2010-10-24

BfIT /Token/

Die Beauftragte der Bundesregierung für Informationstechnik: Was ist ein Token?, http://www.cio.bund.de/cln_164/SharedDocs/FAQs/DE/A/A15.html?nn=586022, Berlin 2010, Abruf: 2010-11-20

BfIT /Verzeichnisdienst/

Die Beauftragte der Bundesregierung für Informationstechnik: Was ist der Verzeichnisdienst?, http://www.cio.bund.de/cln_155/SharedDocs/FAQs/DE/A/A10.html?nn=586022, Berlin 2010, Abruf: 2010-11-20

Bitkom /Online-Banking/

Maurice Shahd: Online-Banking wird zum Standard, http://www.bitkom.org/de/presse/56204_52806.aspx, Berlin 2008, Abruf: 2010-11-25

BMI /Anbindung juristischer Personen/

secunet : Lösungsansätze zur Anbindung juristischer Personen - De-Mail-Gateway für juristische Personen – Version 0.98, http://www.cio.bund.de/SharedDocs/Publikationen/DE/E-Government/anbindung_juristischer_personen_download.pdf?__blob=publicationFile, Berlin 2009, Abruf: 2010-10-24

BMI /De-Mail Informationsbroschüre/

Bundesministerium des Inneren: So einfach wie E-Mail, so sicher wie Papierpost, http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Projekte/de_mail_informationsbroschuere_download.pdf?__blob=publicationFile, Berlin 2010, Abruf: 2010-10-24

BMI /Gesetz/

Bundesministerium des Inneren: Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_Demail.pdf?__blob=publicationFile, Berlin 2010, Abruf: 2010-10-24

BMI /Technische Details/

Bundesministerium des Inneren: Funktionen und technische Details von De-Mail, http://www.fn.de-mail.de/DeMail/DE/01_Buerger/_function/de_mail_technische_details.pdf?__blob=publicationFile, Berlin o. J., Abruf: 2010-10-24

BSI /Infrastuktur/

Bundesamt für Sicherheit in der Informationstechnik: De-Mail – eine Infrastruktur für sichere Kommunikation, https://www.bsi.bund.de/cln_183/ContentBSI/Themen/Egovernment/DeMail/DeMail.html, o. O. O. J., Abruf: 2010-10-24

BSI /Sicherheitsfunktionen/

Bundesamt für Sicherheit in der Informationstechnik: Grundlegende Sicherheitsfunktionen von De-Mail, http://www.cio.bund.de/cae/servlet/contentblob/1143080/publicationFile/90827/sicherheitsfunktionen_download.pdf, o. O. o. J., Abruf: 2010-10-24

BSI /Technische Richtlinie/

Bundesamt für Sicherheit in der Informationstechnik: Technische Richtline – Postfach- und Versanddienst Funktionalitätsspezifikation, https://www.bsi.bund.de/cae/servlet/contentblob/486072/publicationFile/41764/TR_BP_PVD_FU_pdf.pdf, Bonn 2010, Abruf: 2010-10-24

BSI /Technische Richtlinie Identifizierungsdienst/

Bundesamt für Sicherheit in der Informationstechnik : Technische Richtlinie - Funktionalitätsspezifikation Identifizierungsdienst, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/De_Mail/TR_De_Mail_IDL_FU_pdf.pdf?__blob=publicationFile, Bonn 2010, Abruf: 2010-11-25

Bundesministerium der Justiz /UWG/

o. V.: §5 UWG, http://www.gesetze-im-internet.de/uwg_2004/__5.html, Berlin o. J., Abruf: 2010-11-21

Bundesministerium der Justiz /VwGO/

o. V.: §70 VwGO, http://www.gesetze-im-internet.de/vwgo/__70.html, Berlin o. J., Abruf: 2010-11-25

Bundesministerium der Justiz /VwVfG/

o. V.: §3a VwVfG, http://www.gesetze-im-internet.de/vwvfg/__3a.html, Berlin o. J., Abruf: 2010-11-25

Deutsche Telekom /Telekom pusht De-Mail/

o. V.: Deutsche Telekom pusht De-Mail, http://www.telekom.com/dtag/cms/content/dt/de/895456, Bonn 2010, Abruf: 2010-11-20

Gelzhäuser /Pilotprojekt/

Sven Gelzhäuser: Erfolgreiches De-Mail Pilotprojekt: Teilnehmer ziehen Bilanz. In: Datenschutz und Datensicherheit – DuD Ausgabe Volume 34 Nr. 9, Berlin u. a. 2010, S. 646-648

GMX /Einfach wie E-Mail/

o. V.: Einfach wie E-Mail, sicher wie ein Brief, http://service.gmx.net/de/cgi/g.fcgi/products/de-mail, München o. J., Abruf: 2010-11-20

GMX /Häufige Fragen/

o. V.: Häufige Fragen zu De-Mail, http://service.gmx.net/de/cgi/g.fcgi/products/de-mail/faq?sid=babhdec.1290263144.2654.wogqrhdb1o.74.ccg, München o. J., Abruf: 2010-11-20

Govmail.de /Startseite/

o. V.: Startseite, https://govmail.de/modules/kp_suche/index.php, Petershagen o. J., Abruf: 2010-11-20

Halb /Verschlüsselung/

Wolfgang Halb: Verschlüsselung - Theorie und Praxis für den privaten Internetanwender. Norderstedt 2003, S. 16

Haufe /Nachbesserung/

o. V.: Bundesrat forder Nachbesserung am De-Mail-Gesetz, http://www.haufe.de/finance/newsDetails?newsID=1295260449.21&topic=Buchfuehrung&topicView=Buchf%FChrung, Freiburg 2011, Abruf: 2011-01-20

Lapp /Brauchen wir De-Mail/

Thomas Lapp : Brauchen wir De-Mail und Bürgerportale?. In: Datenschutz und Datensicherheit – DuD Volume 33 Nr. 11, Berlin u.a. 2009, S. 651-655

Laudon u.a. /Wirtschaftsinformatik/

Kenneth C. Laudon, Jane P. Laudon, Detlef Schoder: Wirtschaftsinformatik: Eine Einführung. München 2010, S. 1011

Leipold /BGB I/

Dieter Leipold: BGB I: Einführung und allgemeiner Teil. Tübingen 2008, S. 159

Lipski /Social Engineering/

Marcus Lipski: Social Engineering: der Mensch als Sicherheitsrisiko in der IT. Hamburg 2009, S. 7

o. V. /Konferenz Datenschutzbeauftragte /

o. V.: Konferenz der Datenschutzbeauftragten des Bundes und der Länder. In: Datenschutz und Datensicherheit – DuD Volume 33 Nr. 7, Berlin u.a. 2009, S. 424

Oversohl /25 Jahre E-Mail/

Martin Oversohl: 25 Jahre E-Mail in Deutschland. In: Spiegel Online, http://www.spiegel.de/netzwelt/tech/0,1518,639654,00.html, o. O 2009, Abruf: 2010-10-31

Röhm, Fuchs /System-Entwicklung/

Rolf Böhm, Emmerich Fuchs: System-Entwicklung in der Wirtschaftsinformatik.: Systems Engineering. Zürich 2002, S. 543

Roßnagel u. a. /De-Mail und Bürgerportale/

Alexander Roßnagel, Gerrit Hornung, Michael Knopp, Daniel Wilke: De-Mail und Bürgerportale. In: Datenschutz und Datensicherheit – DuD Volume 33 Nr. 12, Berlin u. a. 2009, S. 728-734

Schulz /Rechtsprobleme/

Sönke E. Schulz: Rechtsprobleme des Identitätsmanagements. In: Datenschutz und Datensicherheit – DuD Volume 33 Nr. 10, Berlin u. a. 2009, S. 601-605

Schumacher /Akkreditierung /

Astrid Schumacher: Akkreditierung und Zertifizierung von De-Mail-Diensteanbietern. In: Datenschutz und Datensicherheit – DuD Volume 34 Nr. 5, Berlin u. a. 2009, S. 302-307

Signaturportal.de /Elektronische Rechnungen/

o. V.: Elektronische Rechnungen per E-Mail und SOAP-Webservice, https://www.signaturportal.de/register.php, Spreenhagen 2010, Abruf: 2010-11-20

Spiegel Online /Steuerbetrüger-CD/

Stefan Simons: Steuerbetrüger-CD in Frankreich - Wie Monsieur Falciani mit flüchtigen Millionen jonglierte. In: Spiegel Online, http://www.spiegel.de/wirtschaft/soziales/0,1518,675248,00.html, Hamburg 2010, Abruf: 2010-11-20

T-Systems /Rechtsverbindlich De-Mailen/

o. V.: Rechtsverbindlich De-Mailen, http://www.t-systems.de/tsi/de/910034/Startseite/OeffentlicherSektor/TopStories/Details/2010-07-13-De-Mail, Frankfurt am Main 2010, Abruf: 2010-11-20

WEB.DE /Häufige Fragen/

o. V.: Häufige Fragen - FAQ, https://produkte.web.de/de-mail/haeufige-fragen-faq/, Karlsruhe o. J., Abruf: 2010-11-20

Weyand /Handels- und Gesellschaftsrecht/

Joachim Weyand: Handels- und Gesellschaftsrecht. Ilmenau 2010, S. 20

Weyand /Bürgerliches Recht/

Joachim Weyand: Grundwissen Bürgerliches Recht. Ilmenau 2009, S. 71-72