De-Mail und rechtssichere Kommunikation

Erik Schreiber

angefertigt im Rahmen des Seminars
Wissen in der modernen Gesellschaft

Universität Leipzig
Fakultät für Mathematik und Informatik
Wintersemester 2010/11

Betreuer
Dr. Hans-Gert Gräbe

Inhaltsverzeichnis

1. Einleitung

E-Mails sind schnell und günstig, doch sind sie nicht rechtsverbindlich.

Der Grund: Herkömmliche Mails sind im Grunde nichts weiter als eine Postkarte, deren Inhalt auf dem Weg vom Absender zum Empfänger – theoretisch – von jedem Außenstehenden mitgelesen werden kann.

Die Briefpost – vor allem das Einschreiben – ist im Gegensatz zur E-Mail zwar rechtsverbindlich, aber im Vergleich teuer, aufwändig und zudem langsam.

Nicht zuletzt aus diesen Gründen arbeitet die deutsche Bundesregierung seit 2006 an einen Projekt zur rechtsverbindlichen Kommunikation über das Internet, welches nun kurz vor seiner Fertigstellung steht und bereits im Frühjahr 2011 den Betrieb aufnehmen soll.

Obwohl der Fokus dieser Seminararbeit auf eben diesem Dienst mit Namen „De-Mail“ liegt, setzt sich diese Arbeit zunächst mit dem Begriff der rechtssicheren Kommunikation auseinander. Was bedeutet rechtssichere Kommunikation und was macht diese aus?

Es folgt ein Überblick über gängige Kommunikationsarten, wie z.B. E-Mail, Fax und traditionellem Brief. Neben einer groben Beschreibung werden diese Kommunikationsarten auf ihre Rechtssicherheit untersucht, um den Ansatz des Projekts De-Mail besser verstehen zu können.

Erst daraufhin folgt der eigentliche Kern der Arbeit. Der Dienst De-Mail wird ausführlich beschrieben. Welche Ziele verfolgt der Dienst? Wie ist De-Mail aufgebaut? Welche Funktionen wird De-Mail haben? Auf welche Weise werden die Nachrichten übertragen und welche Sicherheitsvorkehrungen wurden getroffen?

Ziel ist es, dem Leser zunächst ein grundlegendes Verständnis über Struktur und Funktionsweise zu vermitteln, um der später folgenden kritischen Betrachtung des Diensts besser folgen zu können.

Da es neben De-Mail noch weitere – zum Teil sehr ähnliche – Ansätze für rechtssichere Kommunikation gibt, werden diese kurz erläutert. Außerdem wird eine Einschätzung gegeben, inwieweit sich das entsprechende Konkurrenzprodukt mit dem De-Mail-Dienst verwenden lässt oder ihm gefährlich wird.

Anschließend gibt ein chronologischer Verlauf des Projekts De-Mail eine Übersicht über wichtige Meilensteine, wie z.B. die verschiedenen Schritte des Gesetzgebungsverfahrens, den Verlauf des Pilotprojekt oder den Status der Vorregistrierungen.

Schließlich folgt eine kritische Betrachtung mit Vor- und Nachteilen, welche De-Mails aus Sicht des Verbrauchers mit sich bringt. Der Stand dieser Vor- und Nachteile ist vom März 2011. Es ist jedoch wegen entsprechender Planungen abzusehen, dass einige Nachteile in der Zukunft keinen Bestand mehr haben werden. Dies wird an entsprechender Stelle erwähnt.

Da De-Mail nicht nur in der Politik für weitreichende Diskussionen gesorgt hat, werden neben den Vor- und Nachteilen ebenfalls die Fronten der Befürworter und Gegner sowie ihre Argumente skizziert.

In abschließender Betrachtung wird ein Ausblick über die mögliche zukünftige Entwicklung des De-Mail-Projekts und seiner Konkurrenten gegeben. Ferner wird versucht eventuelle Folgen sowohl für Nutzer als allgemein für die Gesellschaft abzuwägen.

2. Was ist rechtssichere Kommunikation?

Eine Kommunikationsart – sei es konventionell per Brief oder digital per E-Mail – ist rechtssicher, wenn sie über eine sichere Rechtskraft verfügt. Das bedeutet, über sie können rechtskräftige, verbindliche Verträge geschlossen werden. Außerdem besitzt sie eine bestätigte Beweiskraft vor Gericht. Ist dies der Fall, spricht man von rechtssicherer Kommunikation.

Um diese Rechtssicherheit zu gewährleisten sind verschiedene notwendige Bedingungen zu erfüllen.

Zum einen ist es wichtig, sowohl Absender als auch Empfänger eindeutig identifizieren zu können. Dies geschieht sowohl bei Briefen als auch bei E-Mails über die gleichnamigen Bezeichnungen Absender bzw. Empfänger. Da jedoch Absender bzw. Empfänger bei E-Mails sich – im Gegensatz zu Briefen – nicht ohne weiteres echten Personen zuordnen lassen, ist hier z.B. keine Rechtssicherheit gegeben.

Ein weiterer notwendiger Punkt um die Rechtssicherheit einer Kommunikationsart zu gewährleisten, ist das Absende- bzw. Empfangsdatum. Vor allem für die fristgerechte Kündigung von Verträgen ist das Absende- bzw. Empfangsdatum unerlässlich.

Bei Briefen dient standardmäßig der Poststempel als Absendedatum, während für ein bestätigtes Empfangsdatum ein Versand als Einschreiben notwendig ist. Bei Verwaltungsakten gilt gemäß §122 Abs.2 Nr.1 Abgabenordnung ein Brief drei Tage nach seiner Absendung als zugestellt. Dies wird als Zustellfiktion bezeichnet.

Bei E-Mails unterscheiden sich zwar Absende- und Empfangsdatum nur geringfügig bis gar nicht, jedoch werden E-Mails von der Zustellfiktion nicht mit eingeschlossen.

Neben den beiden Punkten Absender bzw. Empfänger und Absende- bzw. Empfangsdatum ist es wichtig, den Inhalt der Nachrichten vor Änderungen zu schützen. Bei Briefen erfüllt die Kombination aus versiegeltem Umschlag und Unterschrift weitestgehend diese Bedingung, während E-Mails theoretisch frei lesbar wie Postkarten sind, sofern kein Verschlüsselungsverfahren für den Versand genutzt wird.

Als letzter Punkt spielen die gesellschaftliche Akzeptanz sowie die gesetzliche Grundlage eine Rolle. Selbst wenn eine Kommunikationsart alle vorangegangenen Bedingungen erfüllt, nützt all dies nicht, wenn sie nicht gesellschaftlich anerkannt ist oder die rechtliche Grundlage fehlt. Am Beispiel des E-Mail Versands: Zwar gäbe es mittels Verschlüsselungstechniken und elektronischen Signaturen bzw. Sicherheitszertifikaten die Möglichkeit, E-Mails rechtssicher zu machen, jedoch kann man nur Nutzen daraus ziehen wenn die Gegenseite (bzw. der Gesetzgeber) diese Kommunikationsart als rechtssicheres Mittel anerkennt.

Rechtssichere Kommunikation ist also der sichere, geschützte, verbindliche Versand vertraulicher Nachrichten, wobei die Identität von Absender, Empfänger sowie die Daten bzw. der Zeitraum des Versands zweifelsfrei nachweisbar sind.

3. Kommunikationsformen und ihre Rechtssicherheit

Das offizielle Ziel von De-Mail ist es, eine „verbindliche und vertrauliche“ Kommunikation über das Internet zu ermöglichen.[1] Um einen Überblick zu erhalten, ob und in welchem Ausmaß für eine solche neue Form der rechtssicheren Kommunikation überhaupt eine Nachfrage besteht, werden in diesem Abschnitt zunächst die bisher vorhandenen Kommunikationsarten und der Grad ihrer Rechtssicherheit betrachtet.

3.1 Einschreiben (Brief)

Das Einschreiben stellt im Briefverkehr für den Absender eine Möglichkeit dar, um sich den Versand sowie gegebenenfalls die Auslieferung eines Briefes offiziell bestätigen zu lassen. Zusätzlich zu einer einfachen Versandbestätigung gibt es drei verschiedene Varianten[2] mit zusätzlichen Leistungen: Einwurf, Rückschein oder Eigenhändig.

Beim Einwurf wird zusätzlich zum Versand auch der Einwurf in den Briefkasten oder das Postfach des Empfängers dokumentiert.

Ein Einschreiben mit Rückschein beinhaltet neben der Versandbestätigung noch einen Rückschein mit der Unterschrift des Empfängers, mit welcher er den Erhalt des Briefes bestätigt.

Eigenhändig bedeutet, dass der Brief nur dem Empfänger persönlich (oder einem Bevollmächtigten) übergeben werden darf.

In den Fällen „Eigenhändig“ und „Einwurf“ erhält der Absender keine schriftliche Bestätigung, hat jedoch die Möglichkeit, online den Sendungsstatus zu überprüfen und gegebenenfalls einen Zustellnachweis ausdrucken.

In der Praxis werden die Sendungsnummern jedoch teilweise doppelt vergeben, so dass der Status nicht abgerufen werden kann. („Die Informationen zu Ihrer Sendung sind nicht eindeutig identifizierbar.“)[3]. Auch die Telefonhotline der deutschen Post kann in diesem Fall anscheinend nicht weiterhelfen.[4]

Damit eignen sich sowohl die Einwurf- als auch die Eigenhändig-Variante des Einschreibens als rechtssicheres Kommunikationsmittel, jedoch können doppelte Sendungsnummern dem Absender einen Strich durch die Rechnung machen. Denn ohne den gültigen Nachweis nützt der Versand als Einschreiben nichts.

Im Gegensatz dazu erhält der Absender bei der Variante mit Rückschein eine schriftliche Zustellbestätigung des Empfängers in Form seiner Unterschrift zugeschickt. Jedoch besteht hier die Gefahr, dass der Empfänger nicht angetroffen wird. In diesem Fall hinterlässt der Postbote eine blaue Benachrichtigungskarte mit der Bitte an den Empfänger, die Sendung in der nächsten Postfiliale abzuholen. Zu diesem Zeitpunkt gilt die Sendung jedoch noch nicht als zugestellt. Es liegt also am Empfänger, die Sendung abzuholen und damit dem Absender in die Hände zu spielen oder die Benachrichtigung zu ignorieren. In letzterem Fall ginge die Sendung also nach einer Wartefrist als „nicht zugestellt“ zurück an den Absender.

Somit ist auch diese Variante des Einschreibens an und für sich rechtssicher, kann sich jedoch durch entsprechendes Verhalten des Empfängers als völlig nutzlos erweisen, da die Beweislast beim Absender liegt.

1 http://www.de-mail.de
2 http://www.deutschepost.de/dpag?xmlFile=link1015321_3915
3 http://de.wikipedia.org/wiki/Einschreiben_(Post)
4 http://www.forschungsmafia.de/blog/2006/12/29/die-post-ihre-einschreiben-und-die-einliefernummern/

Häufig wird argumentiert, ein Einschreiben beweise nur den Eingang des Umschlags, nicht jedoch dass überhaupt ein Brief darin enthalten ist. Jedoch sind Mitarbeiter der Post befugt – aber nicht verpflichtet – zu bestätigen, dass ein bestimmtes Dokument per Einschreiben verschickt wurde.

Hierzu muss der Absender sowohl das Originaldokument als auch eine Kopie in der Poststelle vorzeigen. Nach dem Überprüfen der beiden Dokumente auf Gleichheit wird eines kuvertiert und verschickt, das andere erhält einen Bestätigungsstempel für den Absender. Aufgrund des zeitlichen Aufwandes wird diese Zusatzleistung jedoch nur nach eigenem Ermessen der Mitarbeiter angeboten.

3.2 Fax

Im Gegensatz zur E-Mail wird das Fax allgemein im Geschäftsverkehr für einvernehmliche rechtsverbindliche Erklärungen akzeptiert. Jedoch tun sich die Gerichte noch schwer damit, da ein Fax im Grunde eine Bilddatei ist, auch wenn sie eine Unterschrift zeigt.

So ist das Fax für Dokumente, welche eine Unterschrift erfordern (z.B. die Kündigung eines Arbeitsvertrages) vor Gericht nicht zu gebrauchen. Außerdem fehlt beim Fax die Möglichkeit einer aussagekräftigen Sendebestätigung.

Damit ist das Fax kein rechtssicheres Kommunikationsmittel, da es hierbei im Ernstfall an Beweiskraft mangelt.

3.3 E-Mail

Ein ähnliches Problem wie beim Fax stellt sich beim Versand von E-Mails, da es auch hier nicht möglich ist, Unterschriften im herkömmlichen Sinne zu gebrauchen. Zwar besteht die Möglichkeit, Sicherheitszertifikate zu nutzen, doch setzt dies voraus, dass der Empfänger sowohl mit diesen Zertifikaten umzugehen weiß, als auch diese als gültige Unterschrift akzeptiert.

E-Mail ist demnach nur für Dokumente geeignet, welche rechtlich gesehen keiner Unterschrift bedürfen (z.B. Rechnungen) oder wo E-Mails als Kommunikationsmittel vertraglich vereinbart wurden.

Vor Gericht hat eine E-Mail, ebenso wie ein Fax, kaum Beweiskraft. Daher ist die E-Mail in ihrer reinen Form kein rechtssicheres Kommunikationsmittel. An diesem Punkt setzt unter anderen De-Mail an und stellt ein Rahmenkonzept für Absender und Empfänger, um die E-Mail-Übertragung rechtssicher zu gestalten.

3.4 Zeugen

Wenn alles nichts hilft, besteht die Möglichkeit einen Brief, ein Fax oder eine E-Mail unter Zeugen abzusenden bzw. einzuwerfen. Der Zeuge muss lediglich den Inhalt der Nachricht kennen und den Zeitpunkt des Absendens bzw. Einwurfs vermerken.

Steht kein Zeuge zur Verfügung, bietet sich bei Briefen die Möglichkeit, die Nachricht über einen Gerichtsvollzieher zu versenden. Beide Varianten – sowohl über einen Zeugen als auch über einen Gerichtsvollzieher – sind rechtssicher.

Durch die Betrachtungen in 3.1 bis 3.4 der verschiedenen Kommunikationsarten lässt sich erkennen, dass ein Dienst wie De-Mail oder ähnliche Dienste durchaus eine Existenzberechtigung haben und die Grundidee ein fehlendes Puzzlestück in der obigen Betrachtung ergänzen würde.

4. Was ist De-Mail?

Wie in den vorherigen Kapiteln bereits erwähnt wurde, handelt es sich bei De-Mail um eine besondere Form des E-Mail-Versandes zum rechtsverbindlichen und vertraulichen Austausch von elektronischen Dokumenten über das Internet. So sollen zum Beispiel Verträge rechtskräftig gekündigt, Urkunden/Ausweise bei Behörden beantragt oder Rechnungen nachweisbar verschickt werden können.

De-Mail ist ein Projekt der deutschen Bundesregierung in Zusammenarbeit mit mehreren Dienstanbietern[1]. Erstmalig öffentlich wurde De-Mail im November 2008 auf dem IT-Gipfel in Darmstadt vorgestellt. Am 4. Februar 2009 beschloss die Bundesregierung einen entsprechenden Gesetzentwurf[2].

Während das Bundesministerium des Inneren (BMI) die rechtlichen Rahmenbedingungen und die technischen Grundlagen definiert, wird De-Mail von der Privatwirtschaft umgesetzt. Dies geschieht in Form von Providern, welche den De-Mail-Dienst anbieten.

4.1 Ziele

De-Mail wird nach offizieller Aussage „das verbindliche und vertrauliche Versenden von Dokumenten und Nachrichten über das Internet“[3] ermöglichen. Damit würde die E-Mail eine rechtssichere Variante erhalten und könnte unter anderem für Bestellungen, Versicherungsverträge oder Kommunikation mit Behörden genutzt werden.

Zwar würde der Schriftverkehr und das damit verbundene Porto entfallen, doch wird De-Mail im Gegensatz zur E-Mail kein kostenloser Dienst sein. Genaue Preise stehen noch nicht fest, es werden jedoch Kosten in Höhe von 15 bis 20 Cent pro Standard-Brief erwartet. Damit wäre ein Versand noch immer deutlich billiger als über die konventionelle Post oder den E-Postbrief. Hier werden zur Zeit 55 Cent pro Standard-Brief verlangt.

Somit würde neben dem Bürger und den Unternehmen vor allem der deutsche Staat erhebliche Gebühren einsparen können. Sollten 80 Prozent der Behörden in den ersten fünf Jahren an De-Mail teilnehmen, würde dies eine Ersparnis von 20 bis 40 Millionen[4] Euro mit sich bringen.

Offiziell liegt der Fokus des Projekts allerdings auf dem Bürger. Dieser soll mit De-Mail vertraulich, zuverlässig und günstig online kommunizieren können. Zusätzlich soll der Dienst die Kommunikation zwischen Bürgern und Behörden verbessern.

Nicht zuletzt besagt die EU-Dienstleistungsrichtlinie, dass öffentliche Stellen bis Ende 2009 elektronische Kommunikation als verbindliches Medium akzeptieren sollen. De-Mail ist der Versuch der Bundesregierung, diese Richtlinie in nationales Recht umzusetzen.

Die Nutzung des Dienstes soll für den Bürger freiwillig sein, so dass stets eine konventionelle Alternative – z.B. die Briefpost – bleibt.

1 http://www.cio.bund.de/SharedDocs/Projekte/2008/dmail_projekt.html
2 http://www.bundesrat.de/cln_090/SharedDocs/Drucksachen/2009/0101-200/174-09,templateId=raw,property=publicationFile.pdf/174-09.pdf
3 http://www.fn.de-mail.de/DeMail/DE/02_Unternehmen/Unternehmen_node.html
4 http://www.heise.de/newsticker/meldung/Rechtssichere-Buerger-E-Post-De-Mail-Besonderheiten-und-Fallstricke-1037231.html

4.2 Aufbau und Funktionsweise

4.2.1 Provider und Akkreditierung

Der Dienst De-Mail wird nicht staatlich sondern über die Privatwirtschaft betrieben. Diese Provider sind beliehen und werden damit hoheitlich tätig. Allerdings dürfen nur zertifizierte Provider den De-Mail-Dienst ihren Nutzern anbieten.

Für diese Zertifizierung gilt es ein Akkreditierungsverfahren zu durchlaufen. Dieses Verfahren beinhaltet umfangreiche Prüfungen[1] zur Gewährleistung der Sicherheit und Interoperabilität durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). So muss unter anderem sowohl interner als auch externer Zugriff auf die Daten durch Unberechtigte unterbunden werden. Das BSI führt dabei Hackertests durch, kontrolliert das Sicherheitssystem und achtet auf vorliegende Datenschutzsiegel[2].

Diese Bedingungen sind einerseits notwendig, um die Rechtssicherheit des Dienstes und andererseits den reibungslosen Versand von Nachrichten zwischen den verschiedenen Providern zu gewährleisten und Insellösungen zu verhindern.

Zusätzlich muss nachgewiesen werden, dass die datenschutzrechtlichen Anforderungen erfüllt werden. Dies geschieht durch ein entsprechendes Zertifikat des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Hierfür ist dem BfDI vom Provider ein sachverständiges Gutachten vorzulegen. Die Grundlage für dieses Gutachten bildet der veröffentlichte Kriterienkatalog[3] des BfDI.

Ist das Akkreditierungsverfahren erfolgreich bestanden, darf der Provider offiziell am Markt als De-Mail-Provider auftreten und den Dienst anbieten.

Aktuelle Provider sind United Internet (WEB.DE, GMX), die deutsche Telekom (T-Systems,T-Online) und die Mentana-Claimsoft AG. Die deutsche Post plant für ihren E-Postbrief ebenfalls eine Akkreditierung zu beantragen, sobald das De-Mail-Gesetz in Kraft getreten ist[4].

4.2.2 Registrierung und Vorregistrierung

Für De-Mail können sich sowohl natürliche Personen als auch juristische Personen (Firmen, Organisationen, öffentliche Stellen) registrieren. Die Sicherheitsanforderungen bei der Registrierung lassen sich mit denen bei der Eröffnung eines Bankkontos vergleichen.

Für die Registrierung wird vom Benutzer einmalig eine Identifikation verlangt. Bei natürlichen Personen geschieht dies durch Aufnahme diverser Pflichtdaten, wie z.B. Vorname, Nachname, Geburtsdatum, Meldeadresse. Bei juristischen Personen werden sowohl Daten zur juristischen Person selbst als auch die Daten ihrer vertretungsberechtigten natürlichen Personen erfasst.

Im Falle einer natürlichen Person erfolgt diese Identifikation über das Vorweisen eines amtlichen Lichtbildausweises (z.B. Personalausweis), mittels des elektronischen Identitätsnachweises des neuen Personalausweises oder mittels „einer qualifizierten elektronischen Signatur nach § 2 Nummer 3 des Signaturgesetzes“[5]

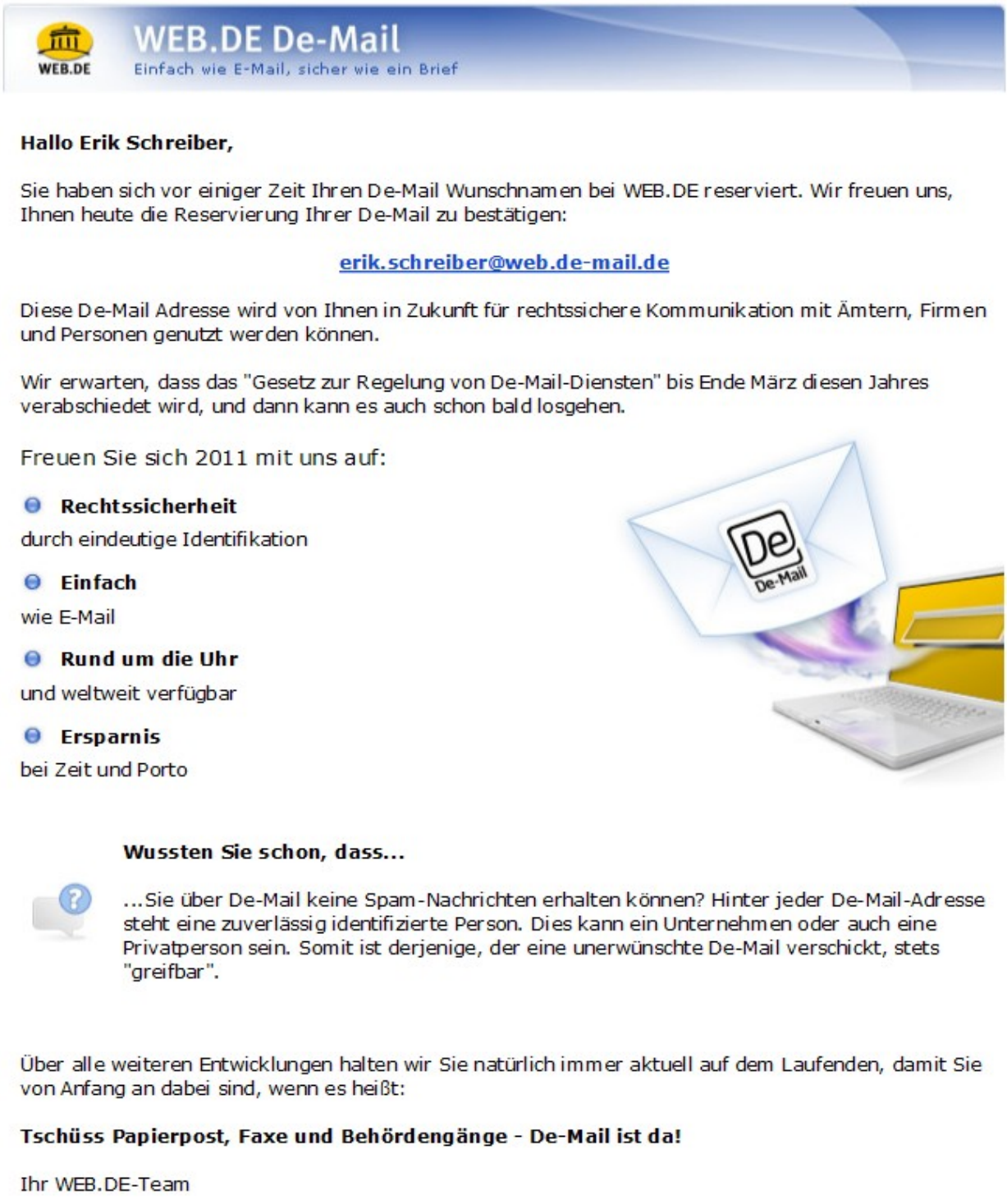
In der Praxis wird wahrscheinlich das Post-Ident-Verfahren für die Identifikation benutzt werden. Jan Oetjen, Geschäftsführer von GMX und WEB.DE, kündigte an, alternativ eine „Authentifizierung nach Terminabsprache kundenfreundlich und komfortabel an der eigenen Haustür oder dem Arbeitsplatz“[6] vorzunehmen.

1 https://www.bsi.bund.de/cln_156/SharedDocs/Downloads/DE/BSI/Egovernment/De_Mail/2010_Mai_DuD_De-Mail_schumacher.html
2 http://heise.de/-817867
3 http://www.bfdi.bund.de/SharedDocs/Publikationen/Orientierungshilfen/DEMailKriterienkatalog.html
4 http://service.deutschepost.de/faq/wie-steht-die-deutsche-post-zum-geplanten-de-mail-gesetz
5 https://www.bsi.bund.de/cae/servlet/contentblob/486036/publicationFile/41750/TR_BP_ACM_FU_pdf.pdf S.10
6 http://www.pressaktuell.de/node/24722

Bei juristischen Personen wird die Identifikation über die Gründungsdokumente (oder gleichwertig beweiskräftige Dokumente), die Einsichtname in die Register- bzw. Verzeichnisdaten oder einen Auszug aus dem Handels- und Genossenschaftsregister (oder vergleichbaren amtlichen Registern bzw. Verzeichnissen) vorgenommen.

Da De-Mail noch nicht offiziell gestartet wurde, ist es momentan noch nicht möglich, sich zu registrieren. Es gibt jedoch die Möglichkeit der Vorregistrierung, um sich seine gewünschte De-Mail-Adresse reservieren zu lassen. (siehe Abbildung 1)

Die Mentana Claimsoft AG begann mit der Vorregistrierung über ihre Domain „signaturportal.de“ bzw. „govmail.de“ bereits am 1. Juli 2010. Kurz danach folgten United Internet über GMX und WEB.DE am 6.Juli 2010, sowie die Deutsche Telekom am 13.Juli 2010.



WEB.DE De-Mail

Einfach wie E-Mail, sicher wie ein Brief

Hallo Erik Schreiber,

Sie haben sich vor einiger Zeit Ihren De-Mail Wunschnamen bei WEB.DE reserviert. Wir freuen uns, Ihnen heute die Reservierung Ihrer De-Mail zu bestätigen:

erik.schreiber@web.de-mail.de

Diese De-Mail Adresse wird von Ihnen in Zukunft für rechtssichere Kommunikation mit Ämtern, Firmen und Personen genutzt werden können.

Wir erwarten, dass das "Gesetz zur Regelung von De-Mail-Diensten" bis Ende März diesen Jahres verabschiedet wird, und dann kann es auch schon bald losgehen.

Freuen Sie sich 2011 mit uns auf:

- **Rechtssicherheit** durch eindeutige Identifikation
- **Einfach** wie E-Mail
- **Rund um die Uhr** und weltweit verfügbar
- **Ersparnis** bei Zeit und Porto

Wussten Sie schon, dass...

...Sie über De-Mail keine Spam-Nachrichten erhalten können? Hinter jeder De-Mail-Adresse steht eine zuverlässig identifizierte Person. Dies kann ein Unternehmen oder auch eine Privatperson sein. Somit ist derjenige, der eine unerwünschte De-Mail verschickt, stets "greifbar".

Über alle weiteren Entwicklungen halten wir Sie natürlich immer aktuell auf dem Laufenden, damit Sie von Anfang an dabei sind, wenn es heißt:

Tschüss Papierpost, Faxe und Behördengänge - De-Mail ist da!

Ihr WEB.DE-Team

Abbildung 1: Bestätigungsmail der Vorregistrierung bei Web.de

4.2.3 Aufbau der Adressen

Eine De-Mail-Adresse setzt sich folgendermaßen zusammen: Nutzer@Domäne

Auf den ersten Blick unterscheidet sich dies nicht von einer herkömmlichen E-Mail-Adresse, jedoch gelten sowohl für den Nutzer als auch für den Domänenteil bestimmte Vorgaben.

Während juristische Personen den Nutzerteil ihrer De-Mail-Adresse ohne Vorgaben wählen können, kann dieser bei natürlichen Personen nur nach zwei Vorschriften gebildet werden:

- <Vorname(n)>.<Nachname>[.<Nummer>]
- <Künstlername / Ordensname>[.<Nummer>]

Die Verwendung des Vornamens ist Pflicht, jedoch steht es dem Nutzer frei, mehrere Vornamen oder eine Abkürzung zu wählen, sofern diese in seinem Personalausweis eingetragen sind. Wenn dieser sich für eine Abkürzung entscheidet, muss diese stets dem abgekürzten Namen entsprechen.

Die Nummer ist optional, wird jedoch bei Mehrfachvergabe des gleichen Namens erforderlich. Dennoch kann der Nutzer in diesem Fall die Zahl frei wählen, sofern diese noch nicht in Kombination mit seinem Namen vergeben wurde.

Neben einer solchem primären De-Mail-Adresse hat der Nutzer die Möglichkeit, weitere pseudonyme De-Mail-Adressen zu beantragen. Hierbei kann im Nutzerteil ein beliebiger Begriff, Name, etc. stehen, welchem stets ein „pn_“ vorangestellt wird. Bedingung neben der Verfügbarkeit der Wunschadresse ist die Einhaltung der moralischen, ethischen und politischen Grundsätze. Außerdem sind reservierte System-Adressen und Adressen die ein „.“ enthalten unzulässig.

Der Domänenteil besteht aus einer Domäne, welche durch den Provider ausschließlich für De-Mail genutzt wird. Damit soll gewährleistet werden, dass eine De-Mail-Adresse auch für Außenstehende sofort als solche erkennbar ist und nicht mit herkömmlichen E-Mail-Adressen verwechselt werden kann. Beispiele für die Bildung des Domänenteils:

- @<provider>.de oder
- @<provider>.de-mail.de (sofern eine Sammeldomäne benutzt wird)

Die Adresse einer Privatperson namens Theo Retisch, welcher sich bei WEB.DE für De-Mail registriert hat könnte also wie folgt aussehen:

- Theo.Retisch.3@web.de-mail.de

während ihm freisteht seinem De-Mail-Konto eine weitere Adresse mit einem Pseudonym hinzuzufügen:

- pn_theorie@web.de-mail.de

Einem De-Mail-Konto können also beliebig viele weitere De-Mail-Adressen zugefügt werden, jedoch verfügt jedes Konto über eine Adresse mit dem tatsächlichen Namen des Inhabers. Das Erstellen mehrerer unabhängiger Konten wird durch die zwingende Identifikation (siehe Kapitel 4.2.2 Registrierung und Vorregistrierung) allerdings nicht möglich sein.

4.2.4 Anmeldung & Authentisierungsniveau

Die Anmeldung am Konto durch den Nutzer erfolgt in zwei Phasen, den sogenannten Authentisierungsniveaus. Das Authentisierungsniveau „normal“ entspricht dem bekannten anmelden per Benutzername und Passwort, wohingegen das Authentisierungsniveau „hoch“ an weitere Bedingungen geknüpft ist und beispielsweise eine bestimmte Chipkarte, den elektronischen Personalausweis oder das Handy (SMS-TAN) erfordert.

Um dieses hohe Authentisierungsniveau zu erreichen, wird eine Zwei-Faktor-Authentisierung bestehend aus „Besitz und Wissen“ notwendig. Damit soll vor Missbrauch durch unberechtigte Kopie des Wissens (z.B. gestohlene Passwörter) oder Diebstahl des Besitzes (gestohlener elektronischer Ausweis oder gestohlenes Handy) geschützt werden.

Nur die Kombination aus beidem ermöglicht das Authentisierungsniveau „hoch“ und schaltet damit alle Funktionen des Kontos frei. Währenddessen beschränken sich die Funktionen im Authentisierungsniveau „normal“ auf unkritische Gebiete, wie z.B. das Lesen von Mails anderer Privatpersonen, nicht aber von Behörden.

Jeder Provider ist dazu verpflichtet, mindestens zwei Verfahren für das Authentisierungsniveau „hoch“ anzubieten. Die eID-Funktion des neuen Personalausweises muss jedoch in jedem Fall ein mögliches Verfahren zur Authentisierung sein.

Das Standard-Authentisierungsniveau, also das Authentisierung mit welchem normalerweise eingeloggt werden soll, kann vom Nutzer in den Einstellungen vorgegeben werden. Alternativ ist ein Wechsel zwischen den Niveaus während der Sitzung über die vom Provider angebotenen Verfahren möglich.

4.2.5 Konto

Jedem De-Mail-Konto wird genau eine Identität zugeordnet, welche bei der Identitätsprüfung bestätigt wird (siehe Kapitel 4.2.2 Registrierung und Vorregistrierung). In jedem Konto werden gespeichert:

- Identitätsdaten des Nutzers
- Informationen zur Authentisierung
- De-Mail-Adresse(n)
- De-Mail-Domain (bei juristischen Personen verpflichtend/bei natürlichen Personen optional)
- Pseudonym-Adressen (nur bei natürlichen Personen)

Jedes De-Mail-Konto kann im Laufe der Zeit verschiedene Zustände annehmen:

- Beantragung
- Reservierung
- Freischaltung
- Sperrung

Ein Konto in Beantragung ist noch kein eigentlich Konto, sondern vielmehr der vorliegende Antrag auf ein De-Mail-Konto mit der unbestätigten Identität des Nutzers und der gewünschten De-Mail-Adresse. Bis Anfang 2011 war dies der Zustand sämtlicher beantragter De-Mail-Konten.

Nach einer positiven Überprüfung durch den Provider, ob die gewünschte Adresse verfügbar ist, gilt ein De-Mail-Konto bzw. eine De-Mail-Adresse als reserviert. Seit Anfang 2011 wurden von den Providern erste Adressen reserviert und die Nutzer darüber informiert (siehe Abbildung 1, Seite 9)

Genutzt werden können die Konten erst, nachdem sie freigeschaltet wurden. Aufgrund der Verzögerung beim De-Mail-Gesetz und dem Gerichtsstreit mit der Deutscher Post wurden bislang noch keine Konten freigeschaltet. Die Freischaltung wird jedoch nicht mehr lange auf sich warten lassen.

Aufgrund eines Verlustes des Authentisierungstokens (Handy, elektronischer Personalausweis, etc.), Missbrauchsverdacht (z.B. bei fehlgeschlagenen Logins durch Probieren oder Brute-Force-Angriff) oder vorsätzlichen Missbrauch (z.B. Spam, moralische Verstöße, etc.) können Konten gesperrt werden. Mögliche Formen sind vollständige Sperrung, Zugangssperre und Nutzungseinschränkung.

Während bei einer vollständigen Sperrung weder Einloggen noch Nachrichtenempfang möglich ist, beschränkt sich die Zugangssperre nur auf ein in der Sperrung definiertes Authentisierungsniveau. Nachrichten können weiterhin empfangen werden. Diese Zugangssperre kann permanenter oder temporärer Natur sein.

Die Nutzungseinschränkung hingegen beschränkt sich nur auf bestimmte Funktionen des Kontos wie den Nachrichtenversand. Einloggen auf allen Authentisierungsniveaus und Nachrichtenempfang sind weiterhin möglich. Diese Form der Sperrung soll unter anderem bei Zahlungsverzug des Nutzers greifen.

Sind die Gründe für die Sperrung beseitigt, kann das Konto gegebenenfalls wieder entsperrt werden.

Neben dem zentralen Dienst von De-Mail, dem Postfach- und Versanddienst, beinhaltet ein De-Mail-Konto eine Dokumentenablage (De-Safe) und einen Identitätsnachweis (De-Ident). Diese drei Komponenten werden in den folgenden Kapiteln näher vorgestellt.

4.2.6 Postfach- und Versanddienst (De-Mail)

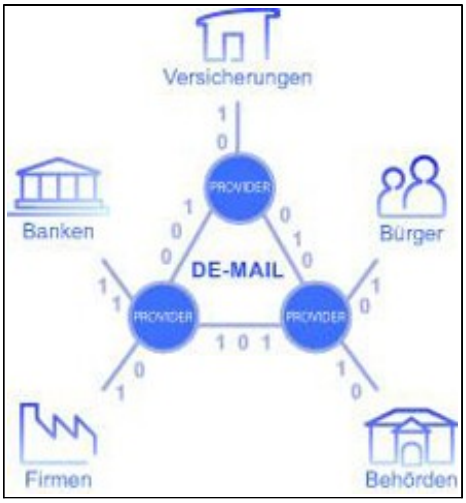


Abbildung 2: Struktur von De-Mail

Über den Postfach und Versanddienst von De-Mail sollen „Bürger, Wirtschaft und Verwaltung zuverlässig und vertraulich elektronisch kommunizieren können.“[1]

Für den Nachrichtenversand stehen dem Nutzer die Varianten „De-Mail“ und „De-Mail-Einschreiben“ zur Auswahl. „De-Mail“ entspricht der Standardnachricht. Diese ist gegen Verlust der Vertraulichkeit sowie gegen Änderungen am Nachrichteninhalt und den Metadaten geschützt.

Das „De-Mail-Einschreiben“ beinhaltet zusätzlich zur Standardnachricht sowohl eine qualifiziert-signierte Bestätigung über Absendedatum der Nachricht als auch über Empfangsdatum im Postfach des Empfängers.

Zusätzlich gibt es bei beiden Varianten die Optionen „Persönlich“, „Absender-bestätigt“, „Versandbestätigung“, „Zugangsbestätigung“ und „Abholbestätigung“ für den Versand.

1 http://www.cio.bund.de/cae/servlet/contentblob/883188/publicationFile/58640/demail_whitepaper_download.pdf

„Persönlich“ bedeutet, dass die Nachricht als persönliche Nachricht eingestuft wird. Damit kann diese vom Empfänger nur gelesen werden, sofern er sich mit Authentisierungsniveau „hoch“ anmeldet.

„Absender-bestätigt“ hingegen bedeutet, dass der Provider des Absender mittels qualifizierter Signatur bestätigt, dass der Absender mit Authentisierungsniveau „hoch“ eingeloggt ist. Es ist abzusehen, dass diese Option für Verträge, Behördengänge, etc. erforderlich sein wird.

Eine Versandbestätigung erzeugt einen Nachweis für den Absender, dass eine Nachricht mit einem bestimmten Inhalt, zu einer bestimmten Zeit an einen bestimmten Empfänger verschickt wurde. Ausgestellt wird sie vom Provider des Absenders.

Eine Empfangsbestätigung erzeugt einen Nachweis für den Absender, dass eine Nachricht mit einem bestimmten Inhalt zu einer bestimmten Zeit im Postfach eines bestimmten Empfängers eingegangen ist. Ausgestellt wird sie vom Provider des Empfängers.

Eine Abholbestätigung erzeugt einen Nachweis für den Absender, dass eine Nachricht mit einem bestimmten Inhalt zu einer bestimmten Zeit in das Postfach eines bestimmten Empfängers eingegangen ist und dieser sich an seinem De-Mail-Konto angemeldet hat. Ausgestellt wird sie vom Provider des Empfängers, der Empfänger muss dabei mit Authentisierungsniveau „hoch“ eingeloggt sein.

Außerdem steht es dem Nutzer frei, seine Nachrichten zusätzlich mit eigenen vorhandenen Komponenten qualifiziert signieren und/oder verschlüsseln zu lassen. Jeder Provider ist dazu verpflichtet, einen entsprechenden Verzeichnisdienst anzubieten, in dem der Nutzer unter anderem auch Verschlüsselungszertifikate zu seinen De-Mail-Adressen hinterlegen kann.

4.2.7 Dokumentenablage (De-Safe)

Die Dokumentenablage kann dazu genutzt werden, um wichtige Dokumente in elektronischer Form aufzubewahren. Hierfür stellt der De-Mail-Provider sogenannte Dokumentensafes zur Verfügung, um eine langfristige Speicherung sowie den Schutz vor Verlust und Manipulation zu ermöglichen. Wie bei Nachrichten werden die übergebenen Dokumente unmittelbar verschlüsselt und integritätsgeschützt.

Die so gesicherten Dokumente sind nach vorangegangener Anmeldung von jedem Ort aus für den Nutzer abrufbar.

4.2.8 Identitätsnachweis (De-Ident)

Der Identitätsnachweis ist eine Möglichkeit anderen Benutzern einen Nachweis über Alter und Identität zu liefern. Hierfür wird vom Provider eine entsprechende Bestätigung generiert und versandt.

Der Nutzer kann sich somit unter anderem bei Online-Shops registrieren oder nachweisen, dass er volljährig ist. Der Nachweis wird vom Provider qualifiziert signiert, um die Korrektheit der übermittelten Daten zu gewährleisten.

Doch nicht nur für Nutzer auch für Onlinehändler oder Website-Betreiber bietet der Identitätsnachweis neue Möglichkeiten. Vor allem im Hinblick auf die gescheiterte Novellierung des Jugendmedienschutz-Staatsvertrages[1], welcher von Website-Betreibern eine Klassifizierung ihrer Inhalte fordern sollte und die damit verbundenen Unklarheiten wie ein Altersnachweis zu erfolgen habe, um vor Gericht anerkannt zu werden, würden hiermit eine bequeme Lösung finden.

1 http://www.heise.de/ct/artikel/Zurueck-auf-Los-1156954.html

4.2.9 Nachrichtenversand & Sicherheit

Durch gegenseitig authentisierte und verschlüsselte Kommunikationskanäle soll die Sicherheit und Vertraulichkeit des Nachrichtenaustauschs gewährleistet werden. Sämtliche Daten, welche durch den Nutzer übertragen oder gespeichert werden, werden umgehend verschlüsselt und integritätsgeschützt.

Verwendet der Nutzer einen Browser, so werden Nachrichten über HTTPS (Hypertext Transfer Protocol via TLS) übertragen. Wird hingegen ein E-Mail-Client benutzt, erfolgt der Nachrichtenversand mittels SMTP (Simple Mail Transfer Protocol) via TLS an den Provider.

Zusätzlich können von Providern auch noch weitere Protokolle, wie z.B. OSCI (Online Service Computer Interface), unterstützt werden, was insbesondere bei Fachverfahren der Verwaltung eingesetzt wird.

Hat der Nutzer eine Nachricht verfasst und Versandoptionen, Empfänger, etc. ausgewählt, wird die Nachricht dem Provider für den Versand überstellt. Dort wird diese zunächst überprüft, bevor sie tatsächlich abgeschickt wird.

Direkt nach dem Eingang der Nachricht beim Provider des Absenders werden ihre Metadaten überprüft (korrekter Absender, korrektes Authentisierungsniveau, etc.). Nachdem die Prüfung erfolgreich beendet wurde, wird der Inhalt der Nachricht auf Malware überprüft. Anschließend werden die Metadaten durch den Provider ergänzt (aktuelle Zeit für Versanddatum) und mit einer Integritätssicherung versehen sowie verschlüsselt.

Die vom Provider des Absenders angebrachte Integritätssicherung besteht aus einer Prüfsumme (Hashwert) über die Metadaten sowie den Nachrichteninhalt. Sollte beim Versand die Versandoption „Absender-bestätigt“ genutzt werden, wird der Hashwert zusätzlich qualifiziert signiert. Die Signatur wird anschließend in den Metadaten der Nachricht gespeichert. Somit wird die korrekte Erfassung der Metadaten und der unveränderte Nachrichteninhalt bestätigt. Anschließend wird der Nachrichteninhalt vom Provider mit einem hybriden Verfahren sowohl für sich selbst als auch für den Provider des Empfängers verschlüsselt.

Falls angefordert, wird vom Provider des Absenders direkt vor der Übertragung der integritätsgeschützten, verschlüsselten Nachricht eine qualifiziert signierte Versandbestätigung ausgestellt. Diese wird anschließend dem Absender als Anhang einer De-Mail zugestellt. In der Bestätigung enthalten sind unter anderem der Hashwert der ursprünglichen Nachricht sowie der Zeitpunkt ihrer Übermittlung. Damit kann der Absender, falls notwendig, sowohl den Versand der Nachricht als auch ihren Inhalt nachweisen.

Die abgeschickte Nachricht wird vom Provider des Absenders mittels SMTP über einen mit SSL/TLS gegenseitig authentisierten und verschlüsselten Kommunikationskanal an den Provider des Empfängers übertragen. Wurde die Nachricht vom Provider des Empfängers entgegen genommen, so wird diese temporär entschlüsselt und die Integrität der Nachricht bzw. der Inhalt unter anderem auf Malware überprüft. Die entschlüsselte Kopie wird nach der Prüfung verworfen, während die Originalnachricht im Postfach des Empfängers abgelegt wird. Dieser Vorgang stellt einen Hauptkritikpunkt an De-Mail dar, da die Ende-zu-Ende-Verschlüsselung unterbrochen wird. (siehe Kapitel 7.2.1 Nachteile & Kritik - Technik)

Ist die Nachricht im Postfach abgelegt, stellt der Provider des Empfängers – sofern gewünscht – eine Zugangsbestätigung für den Absender aus. Die Bestätigung wird wie die Versandbestätigung qualifiziert signiert und als Anhang an den Absender übermittelt. Die Bestätigung enthält unter anderem den Hashwert der ursprünglichen Nachricht und den Zeitpunkt des Empfangsdatums. So kann der Absender wenn nötig nachweisen, dass der Empfänger ab einem bestimmten Zeitpunkt Zugang zur Nachricht hatte.

5. Zeitlicher Verlauf

Dieses Kapitel stellt den zeitlichen Verlauf des Projekts De-Mail grob dar. Von der Projektplanung bis kurz vor Betriebsaufnahme werden wichtige Meilensteine – sowie die Hürden, welche es zu nehmen galt – kurz erläutert.

2006 – Beginn der Arbeiten

Bereits seit 2006 arbeitet das Bundesamt für Sicherheit in der Informationstechnik (BSI) an dem, was heute unter dem Namen De-Mail kurz vor der Einführung steht: Dem Konzept der Bürgermail und der zugehörigen Bürgerportale. (http://heise.de/-210331)

12.07.2007 - Vorstellung des „Konzepts Bürgerportale“

Das Bundesamt für Sicherheit in der Informationstechnik stellt sein Konzept der Bürgerportale als „Mittler zwischen modernen Behörden und ihren Bürger-Kunden“ auf dem CAST-Forum 2007 vor. (http://heise.de/-151081)

09.10.2008 – Erste Kritik

Nach dem Ausscheidens der Strato AG als potentieller Provider ist die Telekom-Tochter T-Systems derzeit der einzige akkreditierte Provider. Strato hatte die Zertifizierung vom BSI nicht erhalten, woraufhin Strato-Geschäftsführer Damian Schmidt De-Mail als „nationalstaatliches Konstrukt“ scharf kritisiert. (siehe hierzu Kapitel 8.1 Befürworter & Gegner)

Inzwischen zählen die Deutsche Bahn, die Deutsche Telekom, die Deutsche Post, Microsoft, der Sparkassenverlag und die Volksbanken zu den Entwicklungspartnern des Projekts De-Mail (http://heise.de/-210331)

20.11.2008 – Erste Öffentliche Vorstellung

Auf dem dritten IT-Gipfel in Darmstadt wird De-Mail erstmals öffentlich durch Kanzlerin Angela Merkel (CDU) vorgestellt. Dem entsprechendem Gesetzentwurf über „Einrichtung und Betrieb von Bürgerportalen“ (Bürgerportalgesetz) wurde bereits vom Bundesinnenministerium erarbeitet. (http://www.golem.de/0810/62846.html, http://heise.de/-206587)

04.02.2009 – Bundeskabinett verabschiedet Bürgerportalgesetz

Das Bürgerportalgesetz wird von der Bundesregierung (Große Koalition) verabschiedet. Das Gesetz regelt die „Einrichtung einer sicheren Kommunikationsplattform“. Das BSI soll durch Überwachung dieser Kommunikationsplattform die Einhaltung der Sicherheitsstandards gewährleisten.

Der Bundesdatenschutzbeauftragte Peter Schaar befürchtet, dass private Nachrichten der Nutzer durch staatliche Dienste über ein Hintertürchen mitgelesen werden könnten. (http://heise.de/-205356)

Das Gesetz wird jedoch in der aktuellen Legislaturperiode nicht mehr vom Bundestag verabschiedet werden können, womit sich der Start von De-Mail weiter verzögert. (http://heise.de/-969880)

Okt. 2009 bis März 2010 – De-Mail-Pilotprojekt

Im Oktober 2009 startet das sechsmonatige Pilotprojekt zu De-Mail im Raum Friedrichshafen. Auf der CeBIT ziehen Internet-Provider, Behörden, Unternehmen sowie Anwender ein „positives Fazit“ aus dem Pilotprojekt. Die Mehrheit wünschte sogar eine Verlängerung des Testlaufs über den März hinaus. 89 Prozent der Tester wollten den Dienst weiter in Anspruch nehmen. (http://heise.de/-817867, http://heise.de/-945382)

Auch das Bundesinnenministerium betrachtet das Pilotprojekt als erfolgreich abgeschlossen und spricht von leicht übertroffenen Erwartungen. Laut Statistik nahmen 40 Unternehmen, Kammern und Behörden sowie 812 Einwohner aus der Testregion teil. (http://heise.de/-969880)

Juni 2010 – Provider starten Vorregistrierung

Die Mentana Claimsoft AG beginnt mit der Vorregistrierung über ihre Domain „signaturportal.de“ bzw. „govmail.de“ bereits am 1. Juli 2010. Kurz danach folgen United Internet über GMX und WEB.DE am 6.Juli 2010 sowie die Deutsche Telekom am 13.Juli 2010. (http://heise.de/-1033628, http://heise.de/-1036940)

Die Provider erwarten eine große Nachfrage bei der Sicherung von De-Mail-Adressen ohne Nummern. (siehe Kapitel 4.2.3 Aufbau der Adressen)

13.10.2010 – Neuer Gesetzentwurf & 700.000 Vorregistrierungen

Da das Bürgerportalgesetz in der vergangenen Legislaturperiode nicht mehr vom Bundestag verabschiedet werden konnte, erarbeitete das Bundesinnenministerium einen überarbeiteten Entwurf[1]. Diesem Gesetzentwurf wird nun von der Bundesregierung (schwarz-gelbe Koalition) zugestimmt. Die Verabschiedung durch Bundestag und Bundesrat steht jedoch noch aus und stellt zwei weitere Hürden des Projekts dar. (http://heise.de/-1107585)

Mittlerweile haben sich nahezu 700.000 Nutzer bei WEB.DE, GMX und der Deutschen Telekom eine De-Mail-Adresse gesichert. (http://www.pressrelations.de/new/standard/result_main.cfm?aktion=jour_pm&r=428281)

November 2010 – Geplanter Start verschiebt sich, Kritik von Bundestag und Bundesrat

Da die Verabschiedung des Gesetzentwurfes sich hinzieht, ist abzusehen, dass De-Mail nicht wie geplant im Januar 2011 starten kann. Neuer Starttermin soll im März 2011 sein. (http://heise.de/-1131022)

Sowohl im Bundestag als auch im Bundesrat stößt der Gesetzentwurf der Regierung auf heftige Kritik. Hauptkritikpunkte sind unter anderem eine fehlende Ende-zu-Ende Verschlüsselung sowie rechtliche und technische Unklarheiten. Die Empfehlungen des Bundesrates umfassen insgesamt 20 Seiten[2]. (http://heise.de/-1135889, http://heise.de/-1140535, http://heise.de/-1143023)

07.12.2010 – Rund eine Million Vorregistrierungen

Trotz Diskussionen und Kritik erreicht die Zahl der Vorregistrierungen die Millionengrenze. Allein 750.000 Nutzer fallen dabei auf WEB.DE und GMX (United Internet).

---

1 http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_Demail.pdf?__blob=publicationFile

2 http://www.bundesrat.de/cln_179/SharedDocs/Drucksachen/2010/0601-700/645-1-10%2CtemplateId%3Draw%2Cproperty%3DpublicationFile.pdf/645-1-10.pdf

08.12.2010 – Gegenäußerung des Bundeskabinetts

Als Entgegnung auf die Empfehlungen des Bundesrates veröffentlicht das Bundeskabinett eine Gegenäußerung[1]. Die Kritikpunkte werden weitestgehend zurückgewiesen.

07.02.2011 – Erneut scharfe Kritik durch Bundestag

Ein Großteil der Experten lehnt das „Gesetz zur Regelung von De-Mail-Diensten“ bei einer Anhörung im Innenausschuss weitestgehend ab. Die Vereinfachung der sicheren Kommunikation im Internet werde zwar begrüßt, jedoch würden die Erwartungen nicht erfüllt werden.

Hauptsächlich werden unter anderem abermals die fehlende Ende-zu-Ende Verschlüsselung und mangelnde Interoperabilität mit bestehenden E-Mail-Standards kritisiert. (http://heise.de/-1184961)

22.02.2011 – Verständigung auf leichte Überarbeitung des Gesetzes

Nach heftigen Diskussion verständigt sich die schwarz-gelbe Koalition auf eine leichte Überarbeitung des Gesetzentwurfs.

Laut den Änderungen müsse eine De-Mail-Domain nicht mehr zwangsläufig den Wortbestandteil „De-Mail“ enthalten, müsse dann aber ausschließlich für De-Mail-Adressen verwendet werden.

(http://heise.de/-1195017)

25.02.2011 – Bundestag verabschiedet De-Mail-Gesetz

Der Gesetzentwurf wird im Bundestag mit den Stimmen der schwarz-gelben Koalition beschlossen. Die Opposition stimmte geschlossen gegen das Gesetz. (http://heise.de/-1197727)

18.03.2011 – Bundesrat stimmt De-Mail-Gesetz zu

Das De-Mail-Gesetz nimmt die letzte Hürde, indem es die Zustimmung vom Bundesrat erhält. Ein vorgelegter Änderungsantrag[2] aus Brandenburg erhielt keine Mehrheit. Nach der Unterzeichnung des Gesetzes durch den Bundespräsidenten sowie der Verkündigung im Bundesgesetzblatt können die Regelungen schon in wenigen Wochen in Kraft treten. Damit können die Provider offiziell ihre Tätigkeit aufnehmen und den De-Mail-Dienst starten. (http://heise.de/-1210572)

1 http://dipbt.bundestag.de/dip21/btd/17/041/1704145.pdf
2 http://www.bundesrat.de/cln_161/SharedDocs/Drucksachen/2011/0101-200/103-1-11%2CtemplateId%3Draw%2Cproperty%3DpublicationFile.pdf

6. Ähnliche Dienste wie De-Mail

Neben De-Mail gibt es weitere Dienste, welche gleiche oder ähnliche Ziele wie das Projekt der Bundesregierung verfolgen. Neben eher unbekannteren Diensten wie eWitness ist der E-Postbrief der Deutschen Post aktuell die wohl größte Konkurrenz für De-Mail. Dieses Kapitel gibt einen knappen Überblick über ähnliche Dienste und stellt diese kurz vor.

6.1 Governikus & EGVP

Das Elektronische Gerichts- und Verwaltungspostfach, kurz EGVP, ist eine javabasierte Anwendung. Über diese ist es möglich, an teilnehmende Gerichte und Behörden Nachrichten sicher und rechtsverbindlich zu übermitteln. Zur Nachrichtenübertragung wird dabei das OSCI-Protokoll (Online Services Computer Interface) genutzt. Optional kann dabei eine elektronische Signatur eingesetzt werden.

Die Software EGVP basiert dabei auf dem OSCI-Client Governikus Communicator, welcher von der Firma „bremen online services GmbH & Co. KG“ (bos KG) entwickelt wurde. Governikus ist eine Middleware, welche in allen deutschen Bundesländern und beim Bund für elektronische Transaktionen im E-Government eingesetzt wird. Mittels Governikus kommunizieren Verwaltung, Unternehmen und Einzelpersonen untereinander über sichere und nachvollziehbare Nachrichten im Internet. Die Entwicklung von Governikus wurde vom Bundesamt für Sicherheit in der Informationstechnik unterstützt.

Das EGVP wird in allen Bundesländern sowie beim Bund auf Seiten teilnehmender Gerichte etc. eingesetzt. Über EGVP können Verfahrensbeteiligte wie Unternehmen, Rechtsanwälte oder Notare Nachrichten übermitteln.

Angewandt wird EGVP zur Kommunikation im Mahnverfahren und mit dem Handelsregister. Für eine Massenkommunikation ist EGVP jedoch nicht ausgelegt. Vielmehr ist es für den internen Verkehr der Justiz optimiert, was eine relativ geringe Benutzerfreundlichkeit zur Folge hat. Außerdem lässt sich EGVP nicht in gängige E-Mail-Programme integrieren.

Nichtsdestotrotz ist das EGVP seit 2004 bei öffentlichen Einrichtungen weit verbreitet. Eine weitere entsprechende Infrastruktur für De-Mail wäre demnach schwierig zu realisieren. Demnach war einer der ersten Kritikpunkte an De-Mail die Inkompatibilität zum EGVP. (siehe Kapitel 7.2.1 Nachteile & Kritik - Technik) Eine Schnittstelle seitens De-Mail ist jedoch bereits geplant, womit sich EGVP und De-Mail miteinander verwenden lassen würden.

6.2 ewitness

Der Service „ewitness“ ist ein elektronischer Notariatsservice. Am Service „ewitness“ sind ausschließlich Notare beteiligt. Der Dienst enthält bereits viele der Leistungsmerkmale des Projekts De-Mail wie verschlüsselter Nachrichtenversand, zertifizierte Nachrichteninhalte und Absendebestätigung.

Das Verfahren wird europaweit zur nachweisbaren, rechtssicheren Durchführung von Onlinetransaktionen mit notarieller Beglaubigung eingesetzt. Da ewitness zudem „nur“ den Zugang zum Server des Empfängers, aber nicht die weitere Behandlung auf Empfängerseite (z.B. Kenntnisnahme oder automatische Spamfiltersortierung) bestätigen kann und wie schon erwähnt nur von Notaren verwendet wird, ist es nicht als Konkurrenz für De-Mail anzusehen.

6.3 E-Postbrief

Nachdem die Deutsche Post ihren E-Mail-Dienst „ePost“ (gestartet im Jahr 2000) Ende Februar 2005 eingestellt hat, probiert sie nun mit dem „E-Postbrief“ einen zweiten Anlauf als E-Mail-Provider.

Wie bei De-Mail können Absender und Empfänger stets eindeutig identifiziert werden. Hierzu nutzt die Deutsche Post bei der Registrierung das hauseigene Post-Ident-Verfahren. Für die Authentisierung kommt ein SMS-TAN-Verfahren zum Einsatz. Auch sonst scheint der Funktionsumfang des E-Postbriefs mit De-Mail mithalten zu können.

Allerdings hat der E-Postbrief aktuell noch einen entscheidenden Vorteil: Während die De-Mail-Provider im Juli 2010 gerade erst mit den Vorregistrierungen begannen, ging der E-Postbrief bereits zu dieser Zeit (14. Juli 2010) an den Start.

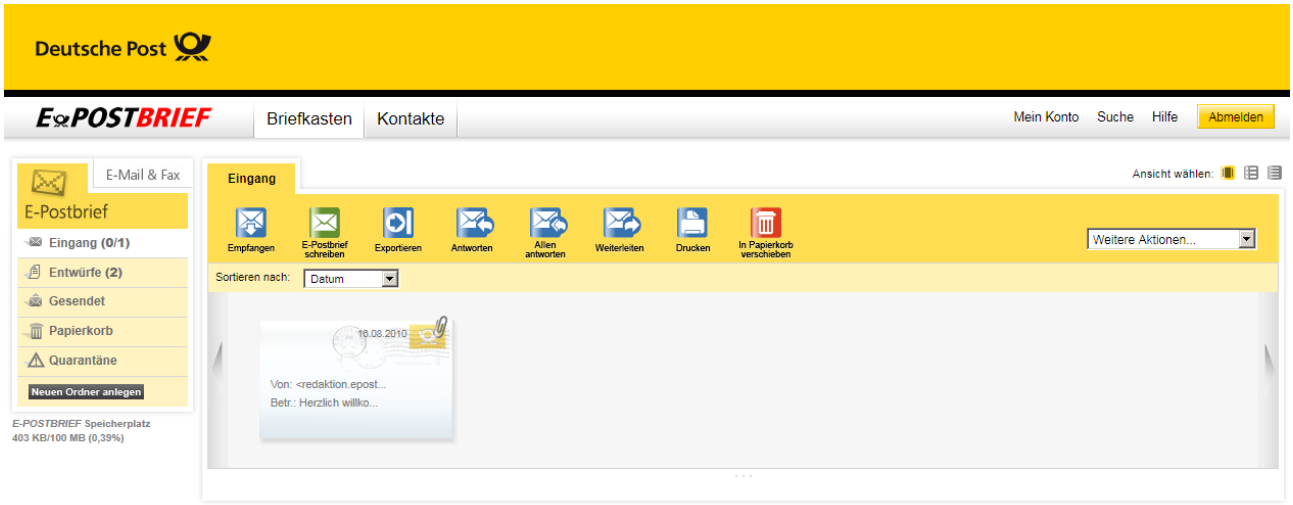


Abbildung 3: E-Postbrief-Postfach

Erstmals angekündigt wurde der E-Postbrief im März 2009. Damals hieß es von Seiten des Konzernsprechers Uwe Bensien, „dass die Post nicht vorhabe, sich am Bundesprojekt De-Mail zu beteiligen“[1].

Entgegen erster Vermutungen fiel der Preis pro E-Postbrief jedoch deutlich höher aus als erwartet.

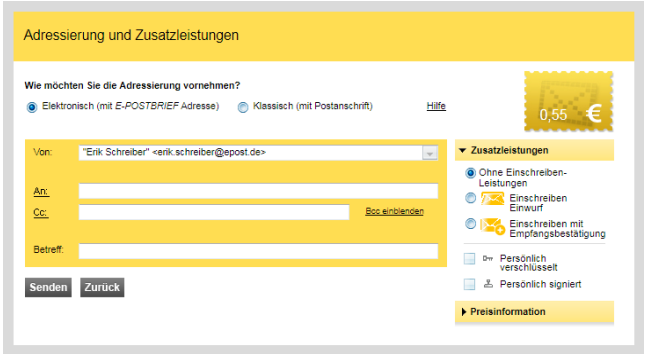


Abbildung 4: Versandoptionen beim E-Postbrief

Hatten Experten im Februar 2010 noch mit ca. 20 Cent pro Mail gerechnet[2], überraschte die Deutsche Post mit einem stattlichen Preis von 55 Cent pro Mail (gleicher Preis wie für einen Standardbrief). Zwar handelt es sich beim E-Postbrief um einen Hybridpostdienst, mit welchem man die E-Mails auch wahlweise als konventionellen Brief zustellen lassen kann (siehe Abbildung 4), jedoch kostet auch eine herkömmliche E-Mail in ein anderes E-Postbrief-Postfach die gleiche Summe.

Es bleibt abzuwarten, wie die Preise sich nach der Einführung von De-Mail entwickeln werden. Für De-Mail wurden Preise zwischen 15 und 20 Cent angekündigt, wenngleich laut United Internet Chef Jan Oetjen auch einstellige Cent-Beträge² denkbar wären.

1 http://heise.de/-206165
2 http://heise.de/-923738

Um den E-Postbrief populär zu machen, wendet die Deutsche Post viel Geld auf. Postwurf-, Plakat-, Online-, Zeitschriften- und sogar Fernsehwerbung wird bemüht, um auf sich aufmerksam zu machen.

Gleichzeitig wächst die Zahl der namhaften Unterstützer des E-Postbriefs: Allianz, ADAC, DekaBank, DFB, Lotto Hessen, Mercedes-Benz Motorsport und SAP. Vertreter von SAP und Allianz waren sogar bei der offiziellen Betriebsaufnahme in Bonn zugegen. SAP kündigte an, den E-Postbrief in seine Personalverwaltung SAP ERP HCM zu integrieren, damit Unternehmen beispielsweise Gehaltsbescheinigungen über den E-Postbrief versenden können. Auch Ebay kündigte an[1], mit der Deutschen Post zusammen zu arbeiten, um Käufer bzw. Verkäufer der Handelsplattform eindeutig zu identifizieren. Dennoch wurde der Unterschied zwischen De-Mail und dem E-Postbrief in der Öffentlichkeit mitunter nicht wahrgenommen.

Was hinter dem E-Postbrief steckt, ist offensichtlich. Die deutsche Post erfährt durch die Verdrängung des traditionellen Briefverkehrs erhebliche finanzielle Verluste. 2009 sanken die Einnahmen allein beim Briefverkehr um 4,9 Prozent auf 13,7 Milliarden Euro. Nun soll der E-Postbrief die Gewinneinbrüche auffangen und die Lebenszeit des traditionellen Briefes künstlich in die Länge ziehen. Entgegen früheren Aussagen hat die Deutsche Post jedoch angekündigt, mit ihrem E-Postbrief einen Akkreditierungsantrag für den De-Mail-Dienst zu beantragen, sobald das De-Mail-Gesetz in Kraft trete.

Trotz aller Mühen sah der E-Postbrief sich bereits keine zwei Wochen nach seiner Einführung mit erheblicher Kritik konfrontiert. So beklagten die Stiftung Warentest sowie Richard Gutjahr – freier Mitarbeiter und Moderator beim Bayerischen Rundfunk – die umständliche Anmeldung für das Verfahren. Außerdem könne – theoretisch – jeder gedruckte E-Postbrief von Mitarbeitern der Post gelesen werden. Aus diesem Grund fallen E-Postbriefe nicht unter den Schutz des Briefgeheimnisses, sondern lediglich unter das Fernmeldegeheimniss. Damit sei die Sicherheit des E-Postbriefes vergleichbar mit der Sicherheit einer Postkarte. Außerdem sei der Dienst unverhältnismäßig teuer.

Weiterhin bestünden die AGBs aus verklausulierten Pflichten, welche dem Kunden auferlegt würden sowie der Weitergabe von Daten an Dritte. Der Kunde ist unter anderem dazu verpflichtet, sein Postfach täglich zu überprüfen. Zudem ergaben erste Tests des Dienstes Unzulänglichkeiten. So erreichten einige der Testmails ihr Ziel erst am zweiten Tag, Druckvorschauen zeigten falsche Bilder und es gab keine Möglichkeit für eine rechtsverbindliche Unterschrift. Die Deutsche Post versicherte daraufhin, die Probleme schnell zu beheben.

Rechtssicher ist der E-Postbrief jedoch nicht. Dies räumte Brief-Vorstand Jürgen Gerdes im März 2010 noch vor dem Start des E-Postbriefes selbst ein[2]. Georg Rau, Mitglied des Bereichsvorstands E-Postbrief, behauptet hingegen Ende 2010, dass der E-Postbrief in „95 bis 99 Prozent aller rechtsgängigen Geschäfte“ rechtssicher sei.

Rechtsanwalt Udo Vetter ist da jedoch anderer Meinung. Dieser bezeichnet die „angebliche Rechtssicherheit“ des E-Postbriefes als „Werbeaussage“. Nur der Gesetzgeber sei in der Lage zu definieren, wann eine E-Mail rechtssicher ist. Die Post hingegen sei aber ein Privatunternehmen.[3]

So bleibt die Rechtssicherheit des E-Postbriefes zweifelhaft. Jedoch dürfte das mit einer Akkreditierung als De-Mail-Provider schnell nachgeholt werden können, wenn es dann soweit ist.

1 http://heise.de/-1201599
2 http://www.netzpolitik.org/2010/e-post-vs-de-mail-es-lebe-das-chaos/
3 http://www.fr-online.de/wirtschaft/kampf-um-die-rechtssichere-e-mail/-/1472780/5030004/-/index.html

7. Vor- und Nachteile von De-Mail

Nachdem in den vorangegangenen Kapiteln sowohl De-Mail als auch andere Möglichkeiten zur rechtssicheren Kommunikation ausgiebig beschrieben wurden, wird De-Mail in diesem Kapitel einer kritischen Betrachtung unterzogen. Welche Vorteile können Nutzer aus der Verwendung von De-Mail ziehen und welchen Nachteilen sehen sie sich gegenüber? Lohnt sich die Nutzung von De-Mail unter dem Strich und wenn ja, zu welchen Kosten?

7.1 Vorteile

Für De-Mail sprechen einige gute Argumente, ist es doch sowohl bequemer als auch auch (voraussichtlich)[1] billiger als ein konventioneller Brief. Man spare neben dem Weg zum Briefkasten und den 55 Cent pro Standard-Brief auch die Kosten für Umschlag, Papier und Druckertinte, so wird auf WEB.DE[2] für den Dienst geworben. Kosten soll das Ganze laut Schätzungen lediglich 15 Cent pro Standard-De-Mail und biete damit allein vom Preis her eine günstige Alternative zur Briefpost.

Alles lässt sich bequem von zu Hause aus erledigen, kein Pilgern zum Postamt ist mehr nötig. Sei es um Briefmarken und fehlende Umschläge zu kaufen oder um den Brief aufzugeben. Allein dies dürfte bei Vielen das Interesse wecken. Damit nicht genug soll De-Mail nicht nur das Briefe schreiben selbst bequemer machen, sondern ebenfalls entsprechende Behördengänge ersparen. So soll sich beispielsweise die Beantragung einer Geburtsurkunde oder Aufenthaltsgenehmigung über De-Mail abwickeln lassen. Damit bliebe einem der Behördengang erspart, was vor allem in Ballungszentren einen nicht zu verachtender Vorteil darstellt. Natürlich entfällt auch die Papierwirtschaft und das Abheften beim Nachrichtenempfang, denn hierfür kann der De-Mail-Safe genutzt werden, welcher seitens des Providers WEB.DE als „sicherer als jede PC-Festplatte“[2] gerühmt wird.

Auch gibt es bei De-Mail keine Leerungszeiten des Postfachs (wie es beim Briefkasten) oder Öffnungszeiten (wie in der Postfiliale). Eine De-Mail kann rund um die Uhr versendet werden, was Vertragskündigungen kurz vor Ende der Kündigungsfrist erleichtern dürfte. Ist die Mail 23:59Uhr am letzten Tag im Postfach des Vertragspartners eingegangen, hat dieser keine Möglichkeit, sich noch herauszureden, soweit die Theorie. Auch benötigt eine De-Mail in der Regel nur wenige Sekunden bis sie beim Empfänger eingeht, während man bei einem Brief mehrere Tage einkalkulieren muss.

Durch ihre Verschlüsselung ist eine Standard-De-Mail zudem auch noch sicherer als eine Standard-E-Mail. Zwar ist es schon seit Jahren möglich, das Sicherheitsmaß einer E-Mail über das aktuelle Maß einer De-Mail zu heben, doch ist dies mit zusätzlichem Aufwand verbunden, für den dem „Otto-Normal-Verbraucher“ entweder das nötige Wissen oder die Zeit bzw. Lust fehlt. Zwar wird bemängelt, dass De-Mail keine Ende-zu-Ende-Verschlüsselung habe, da die Nachrichten temporär zur Überprüfung entschlüsselt werden (siehe Kapitel 7.2 Nachteile & Kritik Seite 22), doch lässt sich dieser Makel durch die Nutzung eigener Verschlüsselungszertifikate wettmachen, welche aus einem Katalog möglicher Zertifikate vom Nutzer ausgewählt werden können.

Nicht zuletzt bietet De-Mail mit De-Ident (siehe Kapitel 4.2.8 Identitätsnachweis (De-Ident) Seite 13) einen bequemen aber aussagekräftigen Altersnachweis, welcher nicht nur für Privatpersonen, sondern auch für Webseitenbetreiber und Onlineshops endlich eine einfache, klare und rechtssichere Möglichkeit der Altersverifikation darstellt, wenn auch nur für deutsche Staatsbürger.

Abschließend betrachtet und im Rückblick auf Kapitel 2 ergänzt De-Mail ein fehlendes Puzzlestück in der rechtssicheren Kommunikation. Zumindest in der Theorie merzt der Dienst die Schwächen anderer Kommunikationsarten aus und vereint ihre Stärken.

1 http://www.email-vergleich.com/2010/02/de-mail-wird-15-cent-pro-e-mail-kosten/
2 https://produkte.web.de/de-mail/vorteile-der-de-mail/

7.2 Nachteile & Kritik

Auf dem ersten Blick scheint De-Mail alles mit sich zu bringen, was sich der deutsche Bürger wünscht. Alles wird einfacher, sicherer, bequemer – zumindest wird der Anschein erweckt. Jedoch trüben einige Wermutstropfen das zunächst strahlende Bild des Dienstes.

Allgemein wird befürchtet, dass Behörden und Unternehmen schrittweise im Laufe der Zeit eine De-Mail zur Voraussetzung für ihre Dienste machen könnten. Daraus würde ein faktischer Zwang zur Benutzung von De-Mail entstehen, auch wenn die Verwendung des Dienstes im Grunde freiwillig ist.

Auch kritisiert Ralf Armbruster aus der Stuttgarter Kommunalverwaltung, dass die Regierung den falschen Weg eingeschlagen habe. „E-Mail ist langfristig nicht die Lösung“ so Armbruster. Denn eigentlich würden die Bürger überhaupt nicht so viele elektronische Nachrichten mit den Behörden austauschen. Eigentlich gehe der Trend mehr in Richtung webbasierter Verfahren, die mit Verschlüsselungszertifikaten arbeiten.

7.2.1 Technik

Wie bereits zuvor erwähnt, stellt die Verschlüsselungstechnik keine Ende-zu-Ende-Verschlüsselung dar. Das bedeutet, eine verschlüsselte Nachricht ist auf ihrem Weg vom Absender aus zum Postfach des Empfängers mindestens einmal unverschlüsselt.

Der Zeitpunkt, zu dem dies geschieht, ist der Eingang der Nachricht beim Provider des Empfängers. (siehe Kapitel 4.2.9 Nachrichtenversand & Sicherheit) An diesem Punkt wird die Nachricht vom Provider kopiert und automatisch entschlüsselt, um auf veränderten Nachrichteninhalt sowie auf Spam, Phishing bzw. Schadsoftware zu prüfen.

Zwar wird die entschlüsselte Nachricht anschließend verworfen, doch besteht prinzipiell die Möglichkeit, dass die Nachrichten von Mitarbeitern des Providers gelesen oder sogar verändert werden. Dies würde zu einem Bruch des Fernmeldegeheimnisses führen. Rechtlich gesehen würde dann die ursprüngliche Nachricht als zugestellt gelten, wobei die veränderte Nachricht im Postfach des Empfängers endet.

Dies kann jedoch verhindert werden, indem der Nutzer zusätzlich eigene Verschlüsselungstechniken aus einem vom Provider angebotenen Katalog wählt. Nur dann existiert eine Ende-zu-Ende-Verschlüsselung.

Ein weiterer Kritikpunkt ist der Spamfilter bzw. der Virenscanner. Ein solcher arbeitet niemals zu 100 Prozent korrekt, Fehler müssen einkalkuliert werden. Ferner sind solche Systeme, welche automatisch jede Mail öffnen können müssen, ein idealer Einstiegspunkt für potentielle Angreifer.

Was nun, wenn Nachrichten fälschlicherweise als Spam oder virenbehaftet markiert werden? Hierfür gibt es nur zwei Möglichkeiten, entweder wird die Nachricht gelöscht oder mit einer entsprechenden Warnmeldung dennoch im Postfach des Empfängers abgelegt.

Wird eine fälschlicherweise als Spam markierte Nachricht also nicht weitergeleitet, so wäre dies eine strafbare Nachrichtenunterdrückung laut §206 StGB. Noch schlimmer wäre der umgekehrte Fall. Eine fälschlicherweise als virenfrei markierte Nachricht (z.B. ein Bußgeldbescheid vom Ordnungsamt) wird im Postfach des Empfängers abgelegt und die Zustellung dem Ordnungsamt bestätigt.

Was nun, wenn der unerkannte Virus beim Öffnen der Nachricht den PC des Empfängers funktionsuntüchtig macht? Trotz Zustellbestätigung könnte die Nachricht dann nicht gelesen werden und weitere unverschuldete Bußgelder, wenn nicht schlimmeres, wären die Folge, liegt die Beweislast in einem solchen Fall doch beim Empfänger.

Wie genau vorgegangen wird, wenn dieser Prüfschritt durch den Virenscanner bzw. den Spamfilter fehlschlägt, ist in den bisher verfügbaren Unterlagen nicht enthalten. Die offizielle Aussage dazu

besagt, „dass hier kein Problem auftreten kann, weil alles auf Servern passiert, die staatlich überprüften Sicherheitsstandards entsprechen und gegen Missbrauch abgeschottet sind“[1]. Was geschieht, wenn dies eben doch möglich ist bleibt vorerst unklar.

Außerdem mangelt es De-Mail, wie in Kapitel 6.1 schon angedeutet, noch an einer Schnittstelle zum EGVP (Elektronisches Gerichts- und Verwaltungspostfach).

EGVP wird bereits seit 2004 in öffentlichen Einrichtungen verwendet. Eine weitere entsprechende Infrastruktur für De-Mail wäre demnach schwierig zu realisieren.

Aus diesem Grund ist eine Schnittstelle zwischen De-Mail und EGVP bereits geplant. Es fanden bereits „Gespräche zwischen Vertretern der AG IT-Standards der Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz und des De-Mail-Projekts“[2] statt. Das „hohe IT-Sicherheitsniveau der Kommunikation über EGVP“[2] solle dabei beibehalten werden.

Des Weiteren wird es nicht möglich sein, von einem De-Mail-Konto aus Nachrichten an reguläre E-Mail-Adressen zu senden. Für den normalen (kostenfreien) E-Mail-Versand wird also ein eigenständiges Konto benötigt.

7.2.2 Datenschutz

Im Gegensatz zu regulären E-Mail-Konten ist die Identität des Nutzers bei De-Mail rechtlich bestätigt. (siehe Kapitel 4.2.2 Registrierung und Vorregistrierung) Diese Identifizierung macht es unmöglich, verschiedene De-Mail-Konten mit voneinander unabhängigen Identitäten anzulegen, da alle Daten des Nutzers an einer zentralen Stelle zusammenlaufen.

Diese hinterlegten Daten des Nutzers können von etlichen Sicherheitsbehörden und Geheimdiensten auch ohne richterliche Anordnung angefordert werden (§113 TKG). Des Weiteren sind über 1000 Behörden in der Lage, die Identität hinter einem De-Mail-Konto online abzurufen. (§112 TKG).

Das De-Mail-Gesetz geht mit seinem §16 noch einen Schritt weiter und sieht die Herausgabe der Identität des Postfachinhabers nach Anfrage von Privatpersonen vor. Ein Umstand, der für die Post oder reguläre E-Mail-Provider eine schwere Datenschutzverletzung darstellen würde.

Ferner wird eine Vorratsdatenspeicherung des Nachrichtenverkehrs bei De-Mail vom Gesetz nicht ausgeschlossen.

Doch nicht nur die Daten des Nutzers können eingesehen werden. Ebenfalls laut §113 TKG sind Kennung und Passwort zu einem De-Mail-Postfach auf Anforderung von einer Strafverfolgungsbehörde, einer Polizeibehörde, des Bundesamtes für Verfassungsschutz, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes herauszugeben. Auch in diesem Fall ist keine richterliche Anordnung von Nöten.

Zwar besteht dieses Recht auch bei regulären E-Mail-Konten, doch besteht dort die Möglichkeit, anonyme Konten, verschiedene Identitäten oder ausländische E-Mail-Konten zu nutzen. Diese Möglichkeit gibt es bei De-Mail nicht.

Hier wird klar, dass die im Postfach oder auch im De-Safe gespeicherten Dokumente nicht so sicher lagern, wie behauptet. In Papierform in der eigenen Wohnung wären sie nicht so einfach und ohne richterliche Anordnung einsehbar.

Ironischerweise gibt das Bundesministerium wortwörtlich als Ziel von De-Mail an, „die nicht-anonyme und sichere elektronische Kommunikation zum Normalfall“[3] machen zu wollen. Datenschützer befürchten, dass eben diese eindeutige Identifizierung für jedermann zum Ausschluss bestimmter Kundengruppen genutzt werden könnte, zum Beispiel wegen mangelnder Bonität, schlichtweg Antipathie oder Kritik am Unternehmen.

1 http://www.ct.de/1017074
2 http://www.bundesrat.de/SharedDocs/Drucksachen/2010/0601-700/645-10_28B_29,templateId=raw,property=publicationFile.pdf/645-10%28B%29.pdf
3 http://www.cio.bund.de/cae/servlet/contentblob/63262/publicationFile/4016/egov2_programm_des_bundes_download.pdf S.15 Abs. 3

7.2.3 Umsetzung

Bereits früh in der Entwicklungsphase von De-Mail geriet das Akkreditierungsverfahren für Provider in die Kritik. Nachdem die Strato AG die notwendige Zertifizierung als De-Mail-Provider – trotz vorhandener internationaler ISO-Norm Zertifizierung[1] – nicht erhalten hatte, kritisierte sie scharf die angewandte Zulassungspraxis.

Damals waren mit der Deutschen Telekom und T-Systems lediglich zwei frühere Staatsbetriebe als Provider akkreditiert. United Internet stieß mit GMX und WEB.DE erst später hinzu.

Außerdem machte sich die „Financial Times Deutschland“ Gedanken zur Tatsache, dass gerade die Telekom, welche vor gut zwei Jahren noch wegen mehrerer Datenschutzskandale und einer Überwachungsaffäre Schlagzeilen machte, für die Bürgermail mit ihren vertraulichen Daten zuständig sei[2].

Auch die enge Zusammenarbeit mit dem Innenministerium, welches die Einführung der Online-Durchsuchung angestrebt hat, lässt viele das Projekt skeptisch betrachten.

7.2.4 Rechtliches

In rechtlicher Hinsicht gibt es noch etliche Unklarheiten. Zwar versucht die Bundesregierung mit De-Mail eine rechtssichere Kommunikation über das Internet zu etablieren, welche Beweiskraft De-Mail aber letztendlich vor Gericht hat, muss sich erst noch zeigen. Sollte diese Beweiskraft deutlich geringer als von der Bundesregierung erwartet ausfallen, wäre der Grund für die Nutzung von De-Mail hinfällig und der Briefverkehr würde seine Stellung als einzig rechtssicheres Kommunikationsmittel behalten.

Ebenfalls unklar ist, wer die Beweislast bei Missbrauch trägt. Der „Chaos Computer Club“ geht davon aus, dass diese – wie auch beim Missbrauch von EC-Karten – beim Verbraucher liegen wird[3].

Auch gibt es bislang keine verbindlichen Aussagen zur Veränderung der Zustellfiktion, welche besagt, dass ein Verwaltungsakt innerhalb von drei Tagen nach Aufgabe zur Post als zugestellt gilt. Ob dies in gleicher Form für De-Mail gilt und ob Wochenend- und Feiertage ebenfalls zählen, bleibt unklar.

Innenpolitiker der schwarz-gelben Koalition betonen, dass eine Frist erst zu laufen begänne, wenn der Bürger die entsprechende Nachricht öffne und so eine Abholbestätigung erzeugt würde. Sollte dies längere Zeit nicht geschehen, so hätte die Behörde die Möglichkeit, das Schreiben konventionell per Post zuzustellen. Nur wenn der Bürger „eingewilligt habe, seine Verwaltungsverfahren ausschließlich digital abwickeln zu lassen, gelte eine De-Mail analog zum Briefverkehr ebenfalls nach drei Tagen als zugestellt“[4].

Trotz dieser Aussage bietet das De-Mail-Gesetz jedoch die Möglichkeit Bescheide ohne Empfangsbestätigung (und Abholbestätigung) zu versenden. Dies könnte fatale Folgen haben, sollte ein Bürger nicht regelmäßig sein Postfach prüfen und beispielsweise einen Bescheid nicht lesen. Ob dann tatsächlich eine weitere Zustellung per Brief erfolgt bleibt abzuwarten.

1 http://www.teltarif.de/arch/2008/kw41/s31556.html
2 http://www.ftd.de/politik/deutschland/:Bundes-E-Mail-Die-sicherste-Versuchung/423746.html
3 http://www.sueddeutsche.de/digital/regierungsplaene-zum-it-gipfel-nie-mehr-spam-1.506137-2
4 http://heise.de/-1210572

8. Die Fronten

Seit fast zwei Jahren ist De-Mail nun Gegenstand etlicher Diskussionen. Die Zahl der Befürworter der Bürgermail fällt jedoch im Vergleich mit ihren Gegnern eher gering aus. Etliche Fronten haben sich gebildet und verhärtet, während die Deutsche Post ein Katz-und-Maus-Spiel um die Kunden und ihre Beteiligung an De-Mail betreibt. Letzterem sei deswegen ein eigener Abschnitt in diesem Kapitel gewidmet.

8.1 Befürworter & Gegner

Strato AG

Erste Kritik am Akkreditierungsverfahren wurde bereits Ende 2008 laut, als Strato-Geschäftsführer Damien Schmidt „vor einem nationalstaatlichen Konstrukt wie De-Mail, das im grenzenlosen Internet Probleme mit der Akzeptanz haben werde“[1] warnte. Wie bereits erwähnt wurde der Strato AG die Zertifizierung als De-Mail-Provider verweigert.

Politik

Schon der Gesetzentwurf des Bügerportalgesetzes der großen Koalition sah sich im Frühjahr 2009 heftiger Kritik und Forderungen nach umfangreichen Nachbesserungen ausgesetzt. Mangelnder Datenschutz, mangelnde Sicherheit, sowie ein vorschnelles Akkreditierungsverfahren bemängelten Linke, Grüne und auch die FDP. Letztere sprach sogar von gravierenden Mängeln und hinterfragte, „warum neben bestehenden Technologien zur sicheren Kommunikation ein neues Mammutprojekt aus der Taufe gehoben werden müsste“[2]. Auf Betreiben der FDP hin wurde für De-Mail vom Parlament sogar eine Haushaltssperre in den Haushaltsplan 2010 eingetragen.

Ende 2010 hat sich die Situation jedoch grundlegend gewandelt. Das Bürgerportalgesetz soll nun durch das De-Mail-Gesetz ergänzt werden, der Bundestag streitet jedoch heftig darüber. Statt einer großen Koalition regiert Schwarz-Gelb und die FDP ist nun einer der größten Befürworter des Projekts. Mit Parolen wie „weg von der Generation Aktenordner, hin zur freien digitalen Gesellschaft“, „ein Schritt in die richtige Richtung“ und „mehr Vertraulichkeit, mehr Datenschutz und Unabhängigkeit von aufwändiger Bürokratie“[3] sollte das Projekt noch 2010 abgeschlossen werden.

Unterdessen hagelt es weiterhin Kritik von Linken, Grünen, sowie auch der SPD. Neben weiteren Bedenken wegen des Datenschutzes wird der generelle Nutzen des Projekts für den Bürger angezweifelt, auch wenn der Grundgedanke lobenswert sei und an der Sicherheit sichtbar gearbeitet worden sei.

United Internet

United Internet Geschäftsführer Jan Oetjen äußerte sich Ende 2010 wie folgt: „De-Mail ist technisch ausgereift und bietet die höchsten Sicherheitsstandards für eine rechtssichere Kommunikation. De-Mail nutzt den Bürgern, der Wirtschaft und der öffentlichen Verwaltung. Die zur Zeit diskutierte Gesetzesvorlage bietet einen optimalen Rahmen für den nötigen strukturellen Wandel unserer Kommunikationsgesellschaft.“[4]

Mit WEB.DE und GMX stellt United Internet derzeit ca. 75 Prozent der Vorregistrierungen für De-Mail.

1 http://heise.de/-210331
2 http://heise.de/-215656
3 http://heise.de/-1135889
4 http://home.1und1.de/themen/nachrichten/in-eigener-sache/947055m/gesetzgebung-zur-de-mail/

Deutscher Anwaltsverein & deutscher Notarverein

In einer Stellungnahme[1] hat der deutsche Anwaltsverein Mitte 2010 die geplanten Regelungen des De-Mail-Dienstes kritisiert. Der Verein sehe grundsätzlich gar keinen Bedarf für den Dienst, da rechtssichere Mail bereits heute mittels elektronischer Signaturen möglich sei. Sollte De-Mail aber dennoch eingeführt werden, würde man sich eine klare Regelung wünschen, wonach es für die anonyme Kommunikation im Internet keine Nachteile geben dürfe. Außerdem solle die Regelung einen „Passus enthalten, nach dem weder eine staatliche Behörde noch ein Unternehmen mit Monopolcharakter, noch der Arbeitgeber eines Bürgers diesen über juristische Regelungen zwingen kann, sich ein De-Mail-Konto zu besorgen“[2]

Nur eine Woche später reiht der deutsche Notarverein sich in die Reihen der Kritiker ein. Zusammen mit dem deutschen Anwaltsverein stellt er in einer gemeinsamen Erklärung[3] den Unterschied zwischen postalischen und elektronischen Briefkästen heraus. Bei Letzteren bestünde die Gefahr, dass eine Vielzahl unerwünschter Nachrichten eingeht und diese Überflutung tatsächlich wichtige Nachrichten untergehen lassen würde, so dass diese entweder nicht wahrgenommen oder versehentlich gelöscht werden könnten.

Arbeitskreis Vorratsdatenspeicherung

Einer der erbittertsten Gegner der Bürgermail ist der Arbeitskreis Vorratsdatenspeicherung. Um faktischen Zwang zur De-Mail-Nutzung zu verhindern, müsse der Dienst boykottiert werden, damit er sich nicht durchsetze.

Er zieht das Fazit, von der Benutzung De-Mails könne nur abgeraten werden[4].

Blogs

Wie auch der Arbeitskreis Vorratsdatenspeicherung ruft der Blog „Netzpolitik.org“ zum Boykott gegen De-Mail auf und führt „Sieben gute Gründe gegen De-Mail“[5] an, um den Aufruf zu stützen.

Auch in etlichen anderen Blogs wird das Thema De-Mail kritisch betrachtet. Neben dem fragwürdigen Ruf der Telekom und dem angeblich mangelndem Fachwissen der Beamten wird vor allem der Datenschutz kritisiert.

So hätten Datensafes von Bürgern nichts beim Staat zu suchen. Außerdem solle es dem Bürger überlassen werden, wie viel Privatsphäre er dem Staat offenbare. Begriffe wie „Schnüffelstaat“ und „Schäuble-Mail“ in Anspielung auf die Vorratsdatenspeicherung und Online-Durchsuchung sind an der Tagesordnung und stellen die Kritik zum Teil satirisch dar.

1 http://anwaltverein.de/downloads/stellungnahmen/SN-10/SN-39.pdf
2 http://heise.de/-1045652
3 http://www.dnotv.de/_files/Aktuelles/PressemitteilungDe-MailfrHomepage.pdf
4 http://www.vorratsdatenspeicherung.de/images/Stellungnahme_Datenschutz_und_Datensicherheit_im_Internet.pdf
5 http://www.netzpolitik.org/2010/de-mail-boykottieren/

8.2 Deutsche Post vs. De-Mail

Sollte De-Mail ein Erfolg werden, sieht die Deutsche Post sich einen schwerwiegendem Problem gegenüber. Der Nachrichtenverkehr verlagert sich von traditioneller Briefpost auf den elektronischen Nachrichtendienst, welcher nicht nur billiger als ein Brief ist, sondern obendrein auch noch von anderen Unternehmen betrieben wird. Es geht um Kunden und natürlich um richtig viel Geld.

War die Deutsche Post neben der Deutschen Telekom zunächst noch Teil der Arbeitsgruppe im Innenministerium, welche De-Mail mit entwickelte, entschloss sie sich im Verlauf der Diskussionen stattdessen ein eigenes System – den E-Postbrief – zu entwickeln. Grund hierfür waren wohl die Befürchtungen, mit dem Projekt De-Mail „die eigene Briefpost zu kannibalisieren“[1].

Das Resultat, der E-Postbrief, unterscheidet sich nur geringfügig von De-Mail. Trotz der Bemühungen der Post ist dieser jedoch nicht rechtssicher, deutlich teurer und verlangt vom Nutzer sogar eine tägliche Kontrolle des Postfachs. Dennoch läuft der E-Postbrief bereits seit Mitte 2010, während die De-Mail-Betreiber zu dieser Zeit gerade einmal die Vorregistrierung starteten.

Einziger funktionaler Vorteil des E-Postbriefes war es, dass man eine Nachricht auch als traditionellen Brief zustellen lassen konnte. Um diesen Vorteil auszumerzen, starteten GMX und WEB.DE pünktlich mit ihrer Vorregistrierung ebenfalls einen sogenannten Hybridpostdienst, indem sie die postalischen Subunternehmer Edipost (GMX) bzw. Francotyp-Postalia (WEB.DE) verpflichteten. Die Preise für einseitige Briefe im A4-Format liegen mit 54 Cent[2] genau einen Cent unter dem Preis des E-Postbriefes.

Für die Post gilt es nun, bis zum Start von De-Mail noch möglichst viele Kunden ins Boot „E-Postbrief“ zu holen und dann ebenfalls, wie bereits angekündigt, einen Akkreditierungsantrag für De-Mail zu stellen. Damit wäre sichergestellt, dass die bisherigen E-Postbrief-Kunden nicht zu De-Mail überwandern, nachdem die Bürgermail an den Start gegangen ist. Mittlerweile haben sich über eine Million Kunden beim E-Postbrief registriert. Bei den De-Mail-Providern sind insgesamt die gleiche Anzahl Vorregistrierungen eingegangen. Zeit ist also Geld und je weiter sich der Start von De-Mail verzögert, desto besser für die Deutsche Post.

Stück für Stück erwächst eine Feindschaft aus der bisherigen Konkurrenz. So boykottierte die Deutsche Post den Nationalen IT-Gipfel, da Kanzlerin Merkel den De-Mail-Stand dort besuchte. Außerdem berichtete die Financial Times im September 2009, dass die Deutsche Post AG das Gesetzgebungsverfahren verzögerte, um der eigenen Dienstleistung E-Postbrief einen Startvorteil zu verschaffen.

Die Reaktion seitens De-Mail lässt nicht lange auf sich warten. So mutmaßt die Deutsche Telekom, „dass die Post hinter einer Debatte um Sicherheitslücken der De-Mail steckt“[3], um den Start der Bürgermail weiter zu verzögern. Die Deutsche Post weist diese Vorwürfe zurück.

Postwendend kündigt die Deutsche Post sowohl United Internet als auch der Telekom das Post-Ident-Verfahren zum 1.1.2011. Man wolle ab diesem Zeitpunkt einen Vertrag abschließen, welcher De-Mail ausschließe. Ohne Post-Ident-Verfahren, welches in Deutschland das Standard-Verfahren für Identitätsüberprüfung ist, dürfte es zunächst schwierig werden, die registrierten Nutzer eindeutig zu identifizieren, was eine weitere Verzögerung zur Folge haben dürfte.

Darauf verklagen die Telekom und United Internet am 12.12.2010 die Deutsche Post und werfen dieser vor, die Einführung von De-Mail zu sabotieren. Zeitgleich prüfen die De-Mail-Provider Alternativen zum Post-Ident-Verfahren. Ein Sprecher der Deutschen Post äußerte sich zu den Vorwürfen: „Wir torpedieren nichts, aber wir stehen ja bald im Wettbewerb zueinander.“

1 http://www.ct.de/1017074
2 http://heise.de/-1033628
3 http://www.wiwo.de/unternehmen-maerkte/de-mail-sabotagevorwurf-an-deutsche-post-449975/

9. Aussicht[1]

Die Provider sind bereit, über eine Million Kunden haben sich bereits vorregistriert. Das De-Mail-Gesetz hat – wenn auch unter heftigem Protest der Opposition – sowohl Bundestag, als auch Bundesrat passiert und kann nun in Kraft treten. Eigentlich könnte De-Mail nun starten, wäre da nicht noch der Gerichtsstreit zwischen den De-Mail-Providern und der Deutschen Post. Diese weigert sich nach wie vor, ihr Post-Ident-Verfahren zur Verfügung zu stellen. Mit einer Entscheidung ist frühestens Ende März 2011 zu rechnen[2]. Damit dürfte sich De-Mail weiter verzögern, was der Deutschen Post nur recht sein kann.

Dennoch wird sich der unvermeidliche Start von De-Mail nicht ewig hinauszögern lassen. Es ist fragwürdig, ob der E-Postbrief gegen De-Mail im Wettbewerb bestehen kann. Die mangelnde Rechtssicherheit, unverhältnismäßig strenge Nutzungsbedingungen und nicht zuletzt der hohe Preis von 55 Cent für eine E-Mail sprechen nicht gerade für die Lösung der Deutschen Post. Nicht einmal die Daten des Nutzers sind hier sicherer aufgehoben als bei De-Mail, da die Deutsche Post mit dem E-Postbrief zum Telekommunikationsanbieter geworden ist. Damit unterliegt auch der E-Postbrief dem Telekommunikationsgesetz und öffnet der staatlichen Überwachung Tür und Tor.

Wenn De-Mail also seinen Betrieb aufnimmt, würde auch eine Preissenkung beim E-Postbrief diesen nur unzureichend aufwerten. Ein Akkreditierungsantrag des E-Postbriefes für De-Mail – wie bereits von der Deutschen Post geplant – ist also sehr wahrscheinlich.

Dennoch befindet sich die Deutsche Post in einer Zwickmühle. Denn selbst wenn sie ebenfalls akkreditierter De-Mail-Provider wird, so muss sie sich – als ehemaliger Monopolist – die Kunden, welche bislang ausschließlich Briefe bzw. E-Postbriefe verschicken konnten, nun mit United Internet und der Deutschen Telekom teilen. Wie man es auch dreht und wendet, Gewinneinbrüche durch De-Mail sind vorprogrammiert, die Frage ist nur noch wie hoch diese ausfallen werden.

Am besten stehen die Chancen für United Internet. Das Unternehmen hält mit über 750.000 Vorregistrierungen bei GMX und WEB.DE den Löwenanteil der bisher erfolgten Vorregistrierungen bei De-Mail.

Ob die Unternehmen mit De-Mail aber das Bombengeschäft machen, entscheiden letztendlich die Nutzer. Jährlich werden in Deutschland über 19 Milliarden Briefe verschickt. Etwa die Hälfte davon haben eine juristische Bedeutung und sind somit potentielle De-Mails.

Das Pilotprojekt in Friedrichshafen gibt Grund zur Annahme, dass De-Mail bei den Nutzern Anklang findet und diese den Dienst intensiv nutzen werden. Dass die Nutzer jedoch damals schon von den fraglichen Datenschutzbestimmungen der Bürgermail wussten, ist nicht anzunehmen. Vielleicht wäre das Projekt dann nicht so positiv ausgefallen.

Im Endeffekt muss der Bürger zwischen Bequemlichkeit und dem Schutz seiner privaten Daten wählen. De-Mail macht die Kommunikation mit Behörden billiger, schneller und weniger aufwändig. Dafür muss der Nutzer jedoch die staatliche Überwachung und seine offenbarte Identität in Kauf nehmen.

Diese Grundsatzdiskussion um den Datenschutz findet sich übrigens regelmäßig in den Diskussionen der jüngeren Vergangenheit wieder. Sei es bei den Social Networks wie Facebook und StudiVZ, bei der Vorratsdatenspeicherung oder bei der Online-Durchsuchung.

Zieht man die Social Networks als Vergleich heran, so könnte man mutmaßen, dass De-Mail in nicht allzu ferner Zukunft ein breites Nutzerspektrum haben dürfte. Immerhin sind die Nachteile der Benutzung von Social Networks ebenfalls weitgehend bekannt und dennoch hat dies ihrem Erfolg keinen Abbruch getan. Denn auch hier überwiegt die Bequemlichkeit gegenüber dem Wunsch nach Datenschutz.

1 Dieses Kapitel spiegelt die persönliche Meinung des Autors wider
2 http://www.versandtarif.de/versandratgeber/news.aspx?newsID=684

Nur wenige zogen die Konsequenzen und löschten ihre Profile bei Facebook bzw. StudiVZ. Zwar ist die Zielgruppe bei De-Mail größtenteils eine andere, reifere als bei Social Networks, dennoch ist der Konflikt vergleichbar.

Im Gegensatz zu Privatpersonen müssen sich Unternehmen, Online-Shops, etc. keine großen Gedanken um den Datenschutz machen. Wichtige Dokumente werden ohnehin im eigenen System gespeichert und die Freilegung der Identität hinter der De-Mail-Adresse ist in der Regel sogar gewünscht.

Alles in allem folgt De-Mail jedoch dem allgemeinen Gesellschaftstrend der letzten Jahre und Jahrzehnte. Der Computer integriert sich immer mehr in den Alltag und übernimmt mehr und mehr Aufgaben. Im Zuge dieser Entwicklung ist eine Umsetzung des „Online-Behördengangs“ also nur eine Frage der Zeit gewesen.

Ob De-Mail so erfolgreich wird, dass der Dienst irgendwann nicht mehr wegzudenken wäre, bleibt abzuwarten. Immerhin befürchten jetzt schon viele Kritiker einen sich langsam entwickelnden faktischen Zwang zu De-Mail. Estland hat es bereits vorgemacht, dort besitzt jeder Bürger eine staatliche E-Mail-Adresse, welche sogar auf dem Personalausweis vermerkt ist. Leider bleibt De-Mail vorerst eine rein nationale Lösung ohne europäischen Bezug.

Vielleicht erfährt jedoch auch die reguläre E-Mail durch De-Mail einen spürbaren Aufwind. Sollte sich De-Mail durchsetzen, so könnte unter Umständen die Hemmschwelle für die Benutzung von E-Mails für kleinere Verbindlichkeiten sinken. Immerhin wären die E-Mails im Gegensatz zu De-Mail völlig kostenlos.

Sollte De-Mail sich behaupten, ist vielleicht auch eine baldige Weiterentwicklung des Dienstes denkbar. So könnte man beispielsweise Urkunden statt per De-Mail über ein 1-Klick-Verfahren beantragen. Die anschließende Abrufung und Zusendung der Urkunde würde vollautomatisch erfolgen.

Abschließend betrachtet ist De-Mail ein Projekt mit hohem Potential, welches jedoch leider von staatlicher Überwachung überschattet wird. Der Erfolg De-Mails ist wahrscheinlich, ob und in welchem Ausmaß dieser eintritt bleibt jedoch abzuwarten.

10. Quellenverzeichnis

- Offizielle Projektbeschreibung De-Mail:
  - http://www.cio.bund.de/SharedDocs/Projekte/2008/dmail_projekt.html
- Offizielle Homepage De-Mail:
  - http://www.cio.bund.de/DE/IT-Projekte/De-Mail/demail_node.html
- "Guter Rat“ Artikel über Rechtssicherheit von Kommunikationsmitteln
  - http://www.guter-rat.de/recht/Von_Einschreiben_bis_E-Postbrief_1761897.html
- Einschreiben – Leistungen der deutschen Post:
  - http://www.deutschepost.de/dpag?xmlFile=link1015321_3915
- Erfahrungsbericht mit Einschreiben (doppelte Sendungsnummern)
  - http://www.forschungsmafia.de/blog/2006/12/29/die-post-ihre-einschreiben-und-die-einliefernummern/
- Wikipedia-Artikel zu Einschreiben
  - http://de.wikipedia.org/wiki/Einschreiben_%28Post%29
- Wikipedia-Artikel zu De-Mail:
  - http://de.wikipedia.org/wiki/De-Mail
- Übersicht über technische Vorgaben von De-Mail:
  - https://www.bsi.bund.de/cln_156/SharedDocs/Downloads/DE/BSI/Egovernment/De_Mail/2010_Mai_DuD_De-Mail_schumacher.html
- De-Mail Kriterienkatalog:
  - http://www.bfdi.bund.de/SharedDocs/Publikationen/Orientierungshilfen/DEMailKriterienkatalog.html
- Technische Richtlinien des BSI zu De-Mail (Accountmanagement & Funktionalitätsspezifikationen)
  - https://www.bsi.bund.de/cae/servlet/contentblob/486036/publicationFile/41750/TR_BP_ACM_FU_pdf.pdf
- Funktionen und technische Details:
  - http://www.cio.bund.de/cae/servlet/contentblob/883188/publicationFile/58640/demail_whitepaper_download.pdf
- Nachrichten rund um De-Mail:
  - http://www.heise.de/produkt/De_Mail
  - http://suche.golem.de/search.php?q=de-mail&l=10&x=0&y=0
- Offizielle Seite des E-Postbriefs
  - http://www.epost.de
- Nachrichten rund um den E-Postbrief
  - http://www.heise.de/produkt/E_Postbrief
- Offizielle Seite von „ewitness“
  - http://www.ewitness.eu/de-de/ewitness.aspx
- Offizielle Seite des EGVP
  - http://www.egvp.de/
- Offizielle Seite von Governikus
  - http://www.bos-bremen.de/de/
- Artikel über De-Mail. E-Postbrief und ewitness
  - http://www.fmm-magazin.de/anbieter-rechtssicherer-e-mail-kommunikation-sagen-der-briefpost-ade-finanzen-mm_kat8_id4111.html
- Kritischer Artikel der „ct“ über De-Mail
  - http://www.ct.de/1017074