

# De-Mail in der Warteschleife

## Das deutsche Bürgerportal lässt auf sich warten

Gerhard Kafka

Eigentlich sollte das geplante Bürgerportalgesetz – Voraussetzung für den offiziellen Start von De-Mail – schon verabschiedet sein. Der Pilotversuch in Friedrichshafen ist abgeschlossen und die beteiligten Partner sind des Lobes voll. Warum eigentlich? De-Mail ist unsicher, sehr teuer und kann nach derzeitigem Wissensstand nur hier in Deutschland eingesetzt werden. Einige Provider haben zwar mit der Registrierung von Benutzern begonnen, De-Mail ist heute aber noch nicht am Markt verfügbar. Zum Glück gibt es Alternativen wie G-Mail, den E-Postbrief und Regify.

Anfang Juli haben die zum Konzern United Internet gehörenden Service Provider GMX und Web.de mit der Registrierung von De-Mail-Adressen begonnen. Weil sie nach einem vorgegebenen Schema gebildet und bei Namensgleichheit derselben vom Provider Kundennummern an den Nachnamen angefügt werden, erwarten die Provider eine große Nachfrage, auch wenn De-Mail selbst noch nicht bundesweit starten kann. Dazu muss vorher das Bürgerportalgesetz in Kraft treten, das voraussichtlich vor Ende dieses Jahres verabschiedet wird. Sicher ist, dass bei Vorlage des Gesetzes umgehend eine seit einem Jahr bei der EU-Kommission in Brüssel vorliegende Beschwerde aktiviert werden wird und sich die Einführung von De-Mail dadurch weiterhin verzögern könnte. Eine Woche nach dem Start der Registrierung von De-Mail-Adressen bei GMX und Web.de begann die Deutsche Telekom ebenfalls mit der Vormerkung von authentischen E-Mail-Adressen.

### Wie De-Mail funktionieren soll

Sämtliche Details und Richtlinien zu De-Mail können von der Webseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter [www.bsi.bund.de](http://www.bsi.bund.de) heruntergeladen werden. Diese Informationen sind für Entwickler und Service Provider bestimmt. Interessierte Bürgerinnen und Bürger finden u.a. auf der Webseite des Pilotprojekts [www.fn.de-mail.de](http://www.fn.de-mail.de) eine Reihe von Hinweisen auf Eigenschaften und Funktionen. Der De-Mail-Postfach- und -Versanddienst ist der zentrale Dienst für die zuverlässige und vertrauliche Kommunikation. De-Mail wird ergänzt durch eine vertrauenswürdige Dokumentenablage (De-Safe) und einen zuverlässigen Identitätsnachweis (De-Ident). Über den zentralen Dienst De-Mail

sollen die Anwender zuverlässig und vertraulich elektronisch kommunizieren können. Die sichere Kommunikation basiert im Wesentlichen auf gegenseitig authentifizierten und verschlüsselten Kommunikationskanälen.



Bild 1: Die Deutsche Telekom verspricht sichere elektronische Post für alle

Alle Daten, die der Nutzer zur Übertragung oder Speicherung an einen De-Mail-Dienst übergibt, werden unmittelbar verschlüsselt und integritätsgeschützt.

Mit De-Mail sind verschiedene Versandarten möglich, die auch unabhängig voneinander genutzt werden können:

- De-Mail: Der Versand ist gegen den Verlust der Vertraulichkeit und gegen Änderungen an Nachrichteninhalt und den Metadaten geschützt.
- De-Mail-Einschreiben: Der Absender erhält zusätzlich eine qualifiziert signierte Bestätigung, wann er die Nachricht verschickt hat und wann sie in das Postfach des Empfängers eingestellt wurde.

Weiterhin kann ein Absender folgende Optionen vor dem Versand einer De-Mail wählen:

- Persönlich: Das erforderliche Authentifizierungsniveau des Empfängers (z.B. wegen der besonderen Vertraulichkeit der Nachricht) muss mindestens „hoch“ sein, um die Nachricht lesen zu können.
- Absenderbestätigt: Der De-Mail-Provider des Absenders bestätigt nach Entgegennahme der Nachricht mittels qualifizierter Signatur, dass

er den angegebenen Nachrichteninhalt vom Absender entgegengenommen hat, der sich mindestens mit „hoch“ authentifiziert hat. Der Empfänger erhält so durch die Bestätigungsnachrichten eine höhere Beweiskraft zum Nachweis der Authentizität des Absenders und zur Integrität der Nachricht.

Ferner kann der Absender seine Nachrichten zusätzlich mit seinen eigenen vorhandenen Komponenten (qualifiziert) signieren und/oder Ende zu Ende verschlüsseln. De-Mail-Provider sind verpflichtet, einen Verzeichnisdienst anzubieten, in dem Nutzer unter anderem auch Verschlüsselungszertifikate zu ihren De-Mail-Adressen hinterlegen können.

Da die zuverlässige Erstregistrierung Grundlage der erforderlichen Identifizierbarkeit der Kommunikationspartner ist, werden nur Verfahren akzeptiert, die hohen Sicherheitsanforderungen genügen, beispielsweise über den künftigen elektronischen Personalausweis (nPA) oder per Post-Ident-Verfahren.

Jedem De-Mail-Konto sind eine oder mehrere De-Mail-Adressen mit der speziellen Endung „.de-mail.de“ zugeordnet. Die Adresse einer natürlichen Person setzt sich somit zusammen aus: <Vorname>.<Nachname>@<De-Mail-Provider>.de-mail.de. Kommt ein Name beim gleichen De-Mail-Provider mehrfach vor, wird die Adresse um eine Zahl ergänzt. Die De-Mail-Adresse des Autors könnte also folgendermaßen aussehen: gerhard.kafka@t-online.de-mail.de.

Neben dieser Adresse lassen sich auch weitere, frei wählbare pseudonyme De-Mail-Adressen innerhalb eines bestehenden Kontos anlegen. Diesen wird das Präfix pn\_ vorangestellt, so dass eine solche Adresse z.B. pn\_mickeymouse@providerXYZ.de-mail.de lauten könnte.

### Sicherheit von De-Mail ist fraglich

Wesentlich für den Erfolg von De-Mail soll sein, dass die versprochene Sicherheit auch tatsächlich gewährleistet wird. Grundlage dafür ist ein IT-Rahmen-Sicherheitskonzept, das die

gesamte Infrastruktur mit einbezieht. Das bedeutet: Das Konzept muss auch die Einsatzumgebung und die Art der Nutzung berücksichtigen. Dieses IT-Rahmen-Sicherheitskonzept setzt eine umfassende Analyse der Risiken und des Schutzbedarfs voraus. Es definiert die Anforderungen zur Umsetzung der Sicherheitsziele und empfiehlt konkrete Maßnahmen.

**De-Mail mit WEB.DE**  
Einfach wie E-Mail, so sicher wie ein Brief!

Der verschlüsselte Kommunikationsdienst De-Mail ist eine gemeinsame Initiative der Bundesregierung mit WEB.DE/DMV, der Deutschen Telekom AG und weiteren Partnern. Er ist seit 3 Jahren in Entwicklung und wurde erfolgreich in einem Pilotversuch getestet.

- Rechtverbindliche elektronische Kommunikation mit Unternehmen, Institutionen und Privatpersonen
- Eindeutig identifizierte Kommunikationspartner im geschlossenen Benutzerkreis
- Beweiskräfte wie ein Einschreiben (durch signierte Versand- und Zustellbestätigung)
- Spart Zeit und Briefmarken (weltweit rund um die Uhr "digitale Briefe" verschicken)

Reservieren Sie sich jetzt schnell bei WEB.DE Ihre persönliche De-Mail-Adresse, unverbindlich und kostenlos!

weiter

Bild 2: Mit diesen Argumenten wirbt Web.de für die sichere elektronische Kommunikation – die Kosten dafür bleiben aber ein Geheimnis

Das BSI bringt seine Kernkompetenzen in das Projekt, indem es für das Sicherheits- sowie Zertifizierungskonzept verantwortlich ist. Damit leistet es einen wesentlichen Beitrag zur Umsetzung der Vision einer sicheren und verlässlichen Infrastruktur für eine vertrauliche und verbindliche elektronische Kommunikation.

Wie im Beitrag „Mitleser unerwünscht“ (NET 10/09, S. 41) bereits erwähnt, bestehen laut deutschem Bundesdatenschützer Peter Schaar gravierende Bedenken gegen den Gesetzentwurf. Und nach wie vor besteht die Möglichkeit, dass ein De-Mail-Provider gleichzeitig im Besitz von E-Mail und dem dazugehörigen Schlüssel ist und ggf. den vertraulichen Inhalt mitlesen kann.

In der 3. Sitzung des strategischen Fachbeirates zur Konvergenzentwicklung des Deutschen Verbandes für Post, Informationstechnologie und Telekommunikation e.V. (DVPT) am 18. Mai wurde diese Sicherheitslücke von De-Mail diskutiert: Bei der Übergabe von Provider zu Provider werden die De-Mail und der Schlüssel, um die De-Mail zu öffnen, übergeben. Die daraus resultierende Missbrauchsgefahr stellt ein enormes Problem dar. Dieser Fehler in der Architektur sollte mit höchster Priorität beseitigt werden, damit De-Mail auch tatsächlich Si-

cherheit gewährleisten kann. Die Details dazu wurden Anfang Juli auf den Webseiten der Frankfurter Rundschau, von Focus Online und des Handelsblattes veröffentlicht. Auf diese Veröffentlichungen reagierte der Verband Bitkom am 21. Juli 2010 mit einer Presseinformation zur Sicherheit von De-Mail, in der Bitkom-Präsident Prof. Dr. August-Wilhelm Scheer darauf verweist, dass Sicherheitsbedenken in der Praxis unbegründet seien; gegenüber der bisherigen E-Mail oder dem Einschreiben und Brief in Papierform bedeute die De-Mail einen Quantensprung in puncto Sicherheit. Dies sollte nicht durch unberechtigte Bedenken zerredet werden.

### Vielleicht kommt De-Mail nie

Vor der Einführung regulärer De-Mail-Dienste sind noch viele Hürden zu nehmen. Solche Dienste können erst nach Verabschiedung des Bürgerportalgesetzes – dieses muss vor Inkrafttreten der EU-Kommission vorgelegt werden – angeboten werden. Am 2. Juli wurde nach umfangreichen Konsultationen ein neuer Referentenentwurf veröffentlicht. Er enthält zum einen höchst bedenkliche Passagen und zum anderen verstößt er möglicherweise gegen geltendes EU-Recht.

Zu den nicht akzeptablen Passagen zählt z.B. der § 5, in dem festgelegt wird, dass ein elektronisches Dokument im Sinne des § 130 BGB als zugestellt gilt, wenn es im Postfach des Empfängers hinterlegt wurde. „Ein elektronisches Dokument gilt in den Fällen des Absatzes 5 Satz 2 am dritten Tag nach der Absendung an den vom Empfänger hierfür eröffneten Zugang als zugestellt, wenn der Behörde nicht spätestens an diesem Tag ein Empfangsbekanntnis nach Satz 1 zugeht.“ Die im selben Paragraph genannte Abholbestätigung erscheint dem Bundesverband Digitale Wirtschaft (BVDW) e.V. ([www.bvdw.org](http://www.bvdw.org)) in einer ausführlichen Stellungnahme nicht sinnvoll und sollte seiner Meinung nach gestrichen werden.

Seit dem April 2009 liegt der EU-Kommission eine Beschwerde gegen die De-Mail-Initiative der Bundesrepublik Deutschland vor. Der Beschwerdefüh-

rer ist die Berliner P1 Privat GmbH, Anbieter von Diensten wie G-Mail und Quabb. P1 ist der Meinung, dass das geplante De-Mail-Gesetz in mindestens zwei Punkten gegen EU-Recht verstößt: Die mit De-Mail einhergehende Wettbewerbsverzerrung und internationale Isolation Deutschlands sei weder mit der Dienstleistungsfreiheit des Art. 49 EG-Vertrag (jetzt Art. 56 AEUV – AEUV steht für „Vertrag über die Arbeitsweise der Europäischen Union“) noch mit den in Art. 86 EG-Vertrag (jetzt Art. 106 AEUV) niedergelegten Wettbewerbsregeln vereinbar.

Eine Reihe von konzeptionellen Schwächen lässt vermuten, dass die Akzeptanz von De-Mail eher gering ausfallen wird. Abgesehen von den nicht bekannten Kosten für den Anwender – die Vermutungen liegen bei ca. 15 ct pro E-Mail – sprechen die folgenden Schwächen gegen eine schnelle Marktdurchdringung:

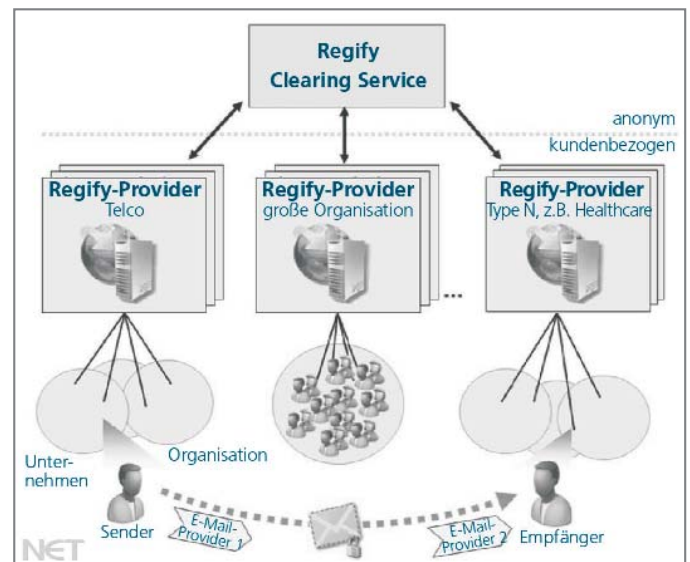
- Die vorgesehene separate De-Mail-Adresse ist kompliziert und aufwendig. Warum sollte ein privater Benutzer oder ein Unternehmen die seit Jahren allen Freunden und Geschäftspartnern bekannte E-Mail-Adresse ändern?
- Durch die Verquickung der Aspekte Netz und Dienst ergeben sich Wettbewerbsprobleme. Der De-Mail-Provider (Dienstanbieter) muss zugleich auch E-Mail-Provider (Infrastrukturanbieter) sein.
- Durch die separate De-Mail-Adresse entstehen Medienbrüche. Parallel zu den häufig eingesetzten E-Mail-Programmen wie Outlook und Lotus Notes muss ein neues Portal benutzt werden.
- Die im De-Mail-Gesetz vorgesehene „Zwangszustellung“ beeinträchtigt die Akzeptanz massiv.
- Das Datenschutzproblem der De-Mail – ein Provider hat E-Mail und dazugehörigen Schlüssel – wird weiterhin für Diskussionen sorgen. Die Aussage des BSI, dass die Sicherheit trotzdem gewährleistet sei, erscheint mehr als zweifelhaft.
- De-Mail ist eine rein deutsche In-sellösung und kann zum jetzigen Zeitpunkt nicht international eingesetzt werden.

- Die Einsparpotenziale werden überschätzt. So stehen den erwarteten Einsparungen zusätzliche Kosten durch neue Stellen im BSI und beim Datenschutzbeauftragten gegenüber. Der größte Kostenblock (rund 18,5 Mio. € jährlich laut Referentenentwurf) ergibt sich durch die Pflicht zur zuverlässigen Identitätsfeststellung bei der Erstregistrierung von Kunden.

### Warum nicht vorhandene Alternativen nutzen?

Wer heute schon sichere E-Mail-Kommunikation betreiben will, kann auf bewährte Lösungen im Markt zurückgreifen, z.B. PGP oder S/MIME (siehe auch NET 10/09, S. 41).

*Bild 3: Das patentierte Regify-Verfahren ist Multi-Provider-fähig und kann im Gegensatz zur De-Mail auch international eingesetzt werden*



(Quelle: Regify)

Der Anbieter P1 Privat ([www.p1privat.de](http://www.p1privat.de)) bietet mit **G-Mail** – nicht zu verwechseln mit Gmail von Google, der diesen Dienst hier in Deutschland als Google Mail anbietet – und Quabb mit De-Mail vergleichbare Dienste an. Wer sich an gezielter Werbung nicht stört, kann hier sogar kostenlose elektronische Briefe versenden. Die Deutsche Post – anfänglich an der Entwicklung von De-Mail beteiligt – hat ein eigenes E-Mail-System entwickelt. Am 14. Juli kündigte sie ihren **E-Postbrief** an. Interessenten können sich ab sofort unter [www.epost.de](http://www.epost.de) für den Dienst registrieren. Um an dem neuen Briefservice teilnehmen zu können, müssen sich Nutzer bei der Erstregistrierung per Post-Ident identi-

fizieren. Für die Anmeldung zum Portal werden Benutzernamen und Passwort benötigt. Zusätzlich erfolgt eine Authentifizierung per TAN-Verfahren über Mobiltelefone. Jeder Brief im Internet ist mit einer qualifizierten elektronischen Signatur der Deutschen Post versehen, die eine Integritätsprüfung der enthaltenen Daten ermöglicht. Unternehmen und Behörden werden über ein gesichertes Gateway angebunden. Dieses Geschäftskunden-Gateway verlangt darüber hinaus, dass sich Unternehmen und das System der Deutschen Post gegenseitig authentifizieren und autorisieren. Der E-Postbrief bis 20 Mbyte kostet 55 ct, die Zusatzleistungen Einschreiben mit Einwurf oder Empfangsbestätigung 1,60 €.

Das weltweit patentierte **Regify-Verfahren** ([www.regify.com](http://www.regify.com)) wird bereits von fünf Providern kommerziell in Deutschland angeboten. Auch die Volksbank Kaiserslautern-Nordwestpfalz eG nutzt den Dienst und ist damit Vorreiter für den gesamten Raiffeisenverbund. Regify gilt mit monatlichen pauschalen Kosten für typisch 200 bis 300 E-Mails pro Benutzer zwischen 3 und 4 € als Kostenführer in diesem Bereich. Die Software ist heute für diverse E-Mail-Clients verfügbar und wird auch für Massenversendungen eingesetzt. Für Anwälte und Kanzleien bietet sich die auf Regify basierende Securamail-Lösung an, die von AC-Systeme offeriert wird. (we)