COMPUTERWOCHE
VOICE OF DIGITAL

De-Mail

Dokumente rechtssicher versenden und archivieren

Datum: 18.01.2012
Autor(en): Thomas Pelkmann

De-Mail erlaubt das Versenden von rechtsverbindlichen Dokumenten. Was genau das ist und wie De-Mail diese Rechtssicherheit garantiert, zeigt der folgende Beitrag.

De-Mail ermöglicht den rechtssicheren Versand von Dokumenten über das Internet. Die ersten Anbieter werden voraussichtlich im März 2012 starten.
Foto: BSI

Phishing[1], **Spoofing**[2], **Spam**[3]: Es gibt gute Gründe für fälschungssichere E-Mail-Accounts. Nicht alle haben mit der mangelnden Sicherheit normaler E-Mail-Adressen zu tun. Sichere Postfächer, deren Absender eine geprüfte Identität besitzen, wären auch deshalb zu begrüßen, weil elektronische Kommunikation einen immer größeren Anteil an der Gesamtkommunikation hat. Angebote, Verträge, Auftragsbestätigungen, Rechnungen, Mahnungen: All diese Schriftstücke entstehen heutzutage fast ausschließlich im Computer. Um sie bisher rechtsgültig zu versenden, ist es nötig, diese Schriftstücke auszudrucken und per Einschreiben auf dem Postweg zu versenden. Die Empfänger scannen diese Dokumente oft genug anschließend ein, um sie im Dokumentenmanagementsystem digital weiterverarbeiten und archivieren zu können.

Diese Medienbrüche erscheinen anachronistisch - besonders dann, wenn man die immensen Kosten berücksichtigt, die dabei entstehen. Beim Absender wird gedruckt, gefaltet, eingetütet und zur Post gebracht, was beim Empfänger wieder ausgepackt, gescannt, gebucht und archiviert wird. Arbeitszeit, Druckkosten, Porto: Da kommt einiges zusammen, was man sich sparen könnte.

Eine Studie der Europäischen Kommission hat Einsparungen von 72 Prozent beim Wechsel von der herkömmlichen Papierrechnung zur elektronischen Rechnung ausgerechnet, **berichtete 2009 die Computerwoche**[4]. In einer weiteren Untersuchung wurde ermittelt, dass eine per Post versendete Rechnung im Durchschnitt mit 16,16 Euro zu Buche schlägt, während der Gesamtprozess des standardisierten Datenaustauschs ganze zwei Euro kostet.

So ist es logisch, dass Gesetzgeber und Branchenverbände daran arbeiten, den rechtssicheren, elektronischen Versand von Dokumenten zu ermöglichen. Die Bundesregierung hat dafür im April 2011 das De-Mail-Gesetz beschlossen, das den sicheren, vertraulichen und nachweisbaren elektronischen Versand von Dokumenten regelt. Das Gesetz ist eine nationale Umsetzung der europäischen Dienstleistungsrichtlinie, die Behörden verpflichtet, eine rechtssichere, elektronische Kommunikation zuzulassen. Seitdem arbeiten verschiedene Provider daran, als Anbieter zugelassen zu werden und De-Mail-Dienste anzubieten. Die ersten De-Mail-Provider werden voraussichtlich in der ersten Jahreshälfte 2012 ihre Dienste starten.

Was ist eigentlich rechtssichere Kommunikation?

Kurz gesagt, bedeutet rechtssichere Kommunikation, dass die Identität von Absender und Empfänger geprüft wird und bekannt ist und dass ein Dokument in einer integren Form nachweislich zugestellt wird.

Im normalen Briefverkehr ist ein ausgedruckter und unterschriebener Brief ein Dokument im Rechtssinne: Es ist signiert und lässt sich nicht ohne weiteres verändern. Eine sichere Zustellung erreicht man über das Einschreibe-Verfahren, bei dem der Zusteller sich vom Empfänger den Erhalt eines Briefes schriftlich bestätigen lässt. Zudem kann der Absender über den Einlieferungsbeleg nachweisen, dass er das Dokument zu einem bestimmten Datum abgeschickt hat.

Der Nachteil dieses Verfahrens: Man kann zwar nachweisen, dass man einen ein Brief verschickt hat, der auch empfangen wurde. Aber einen Nachweis über den tatsächlichen Inhalt eines Schreibens gibt es darüber nicht.

Diese Rechtsunsicherheit führt bei deutschen Gerichten oft dazu, dass den Einschreibebelegen keine Beweiskraft zugebilligt wird. "Der vom Empfänger unterzeichnete Empfangsbeleg begründet die Vermutung, dass zu dem im Rückschein genannten Datum eine Sendung zugestellt wurde", heißt es dazu bei Wikipedia. Und weiter: "Ein voller Beweis des Zugangs eines Schriftstückes mit einem bestimmten Inhalt ist nur mit einer Zustellung durch einen Gerichtsvollzieher möglich, § 132 BGB, die jeder in Auftrag geben kann."

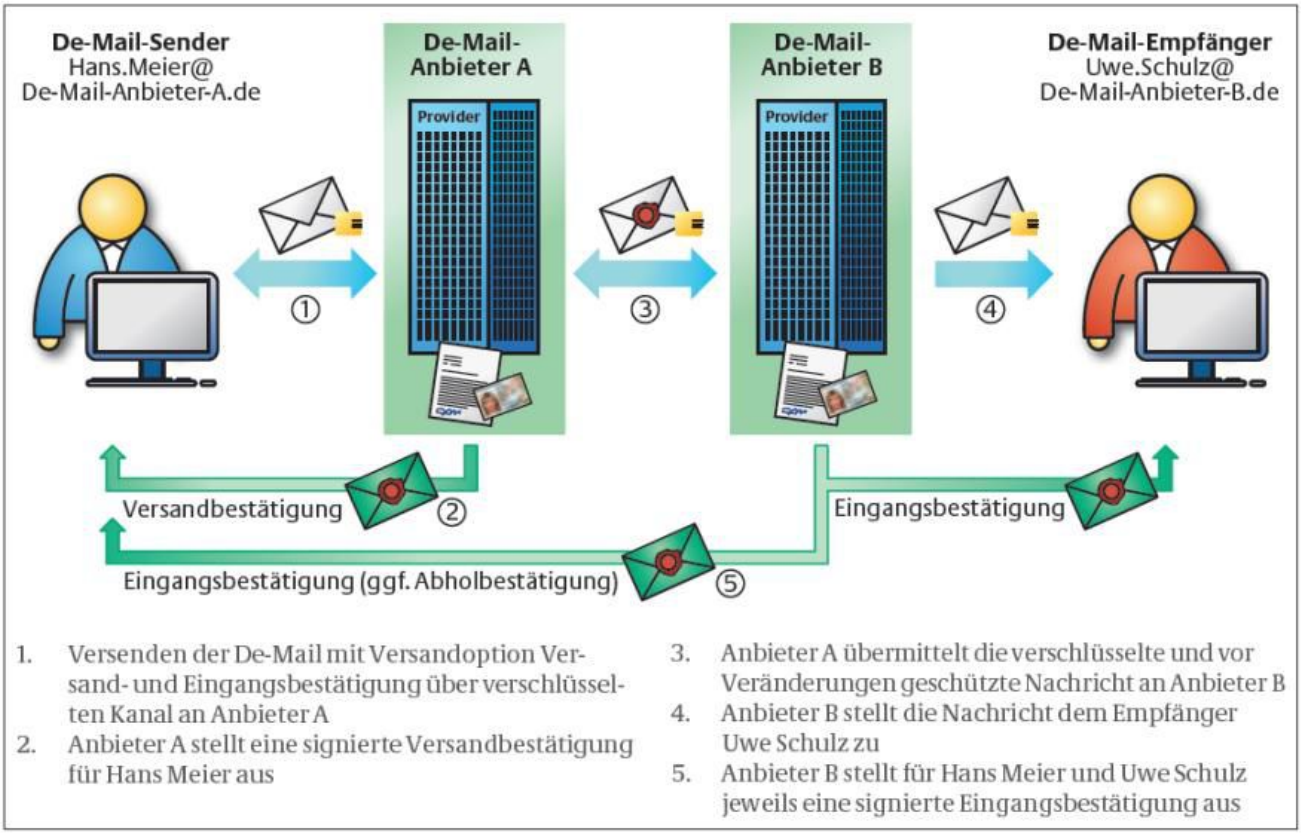
Neben den hohen Prozess- und Verbrauchskosten ist normale Post also auch rechtlich unsicher. Zeit, sich den digitalen Darreichungsformen von Post zuzuwenden.

Was bei De-Mail ist rechtssicher?

E-Mail[5] gehört zu den am häufigsten genutzten Kommunikationsformen überhaupt. Im Jahr 2010 wurden weltweit rund 107 Billionen E-Mails verschickt, allerdings mit einem Spam-Anteil von fast 90 Prozent. Aber selbst, wenn man den Müll rausrechnet, bleiben noch rund 963 Milliarden "richtige" E-Mails übrig. Obwohl E-Mails keine Rechtsverbindlichkeit besitzen, schreibt der Gesetzgeber für den geschäftlichen Mail-Verkehr vor, dass der Absender eine Signatur benutzen muss. Diese elektronische Unterschrift muss unter anderem Angaben über die Firma und die Rechtsform des Unternehmens enthalten, Ort des Firmensitzes sowie die Namen der vertretungsberechtigten Geschäftsführer.

Mit dem Mitte 2011 verabschiedeten De-Mail-Gesetz haben diese Signaturen am Fußende von E-Mails aber nichts zu tun. Bei dem Gesetz geht es darum sicherzustellen, dass eine **De-Mail**[6] von einem eindeutig bekannten und feststellbaren Absender stammt. Dafür ist es nötig, sich bei einem De-Mail-Anbieter als natürliche oder juristische Person zu registrieren und bei der Eröffnung eines Benutzerkontos seine Identität nachzuweisen. Dazu muss man sämtliche Ausweisdaten wie Vor- und Nachname, Meldeadresse und Geburtsdatum angeben. Bei juristischen Personen wie Unternehmen werden zusätzlich auch die Namen der vertretungsberechtigten Personen erfasst.

Mit dieser Registrierung steht und fällt De-Mail; wäre es möglich, hier Identitäten zu fälschen, würde das gesamte System zusammenbrechen. Daher greift man für das Verifizieren von Identitäten auf anerkannte Verfahren wie den elektronischen Personalausweis oder das Postident-Verfahren zurück.



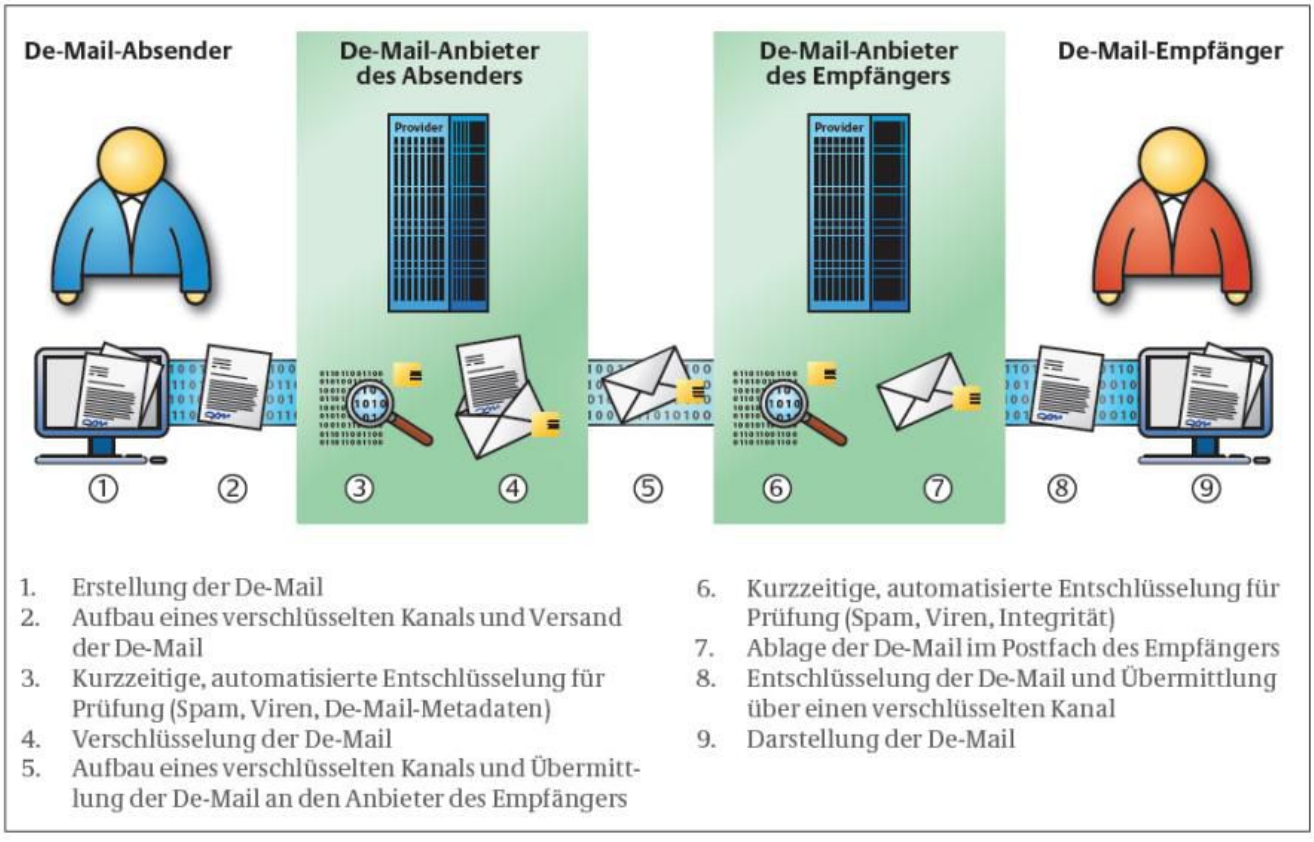
Sicherheit: Versand und Empfang erfolgen nur innerhalb des De-Mail-Verbundes aller De-Mail-Provider. Foto: Bundesamt für Sicherheit in der Informationstechnik

Ebenso wichtig wie die sichere Identifizierung von Absender und Empfänger ist die Sicherung des Transportweges. Es ist nicht nur theoretisch denkbar, dass Mails auf dem Übertragungsweg abgefangen und umgeleitet und danach geändert an den ursprünglichen Adressaten weitergeleitet werden. Um das zu verhindern, setzt De-Mail auf die Verschlüsselung der Daten beim Transport. Dafür setzt De-Mail die so genannte **Transport Layer Security (TLS)**[7] ein, früher unter dem Namen SSL bekannt. TLS sorgt dafür, dass Daten bei der Übertragung so verschlüsselt werden, dass sie von Dritten nicht gelesen und damit auch nicht verändert werden können.

Über dieses Verfahren ist zwar der Transportweg der Daten gesichert, nicht aber die Daten selber. Eine **Ende-zu-Ende-Verschlüsselung**[8] von Dokumenten ist bei De-Mail nicht implementiert, so dass es auf Providerseite prinzipiell möglich ist, eine De-Mail unbefugterweise zu lesen. Bundesregierung und Provider argumentieren beim Verzicht auf die Verschlüsselung der Dokumente unter anderem damit, dass das De-Mail zu kompliziert machen würde, um von Endnutzern angenommen zu werden. Allerdings ist eine Ende-zu-Ende-Verschlüsselung durch die Anwender möglich, wenn sie dies wünschen.

Zugangs- und Empfangsbestätigungen

Anders als bei traditionellen Einschreiben ist es bei De-Mail nicht nur möglich, Versand und Empfang von Dokumenten rechtsverbindlich zu bestätigen. Auch der Inhalt der Dokumente kann rechtsverbindlich dokumentiert werden. "Die Integrität", heißt es dazu beim Bundesamt für Sicherheit in der Informationstechnik (BSI) " wird bei den Nachrichten durch eine Prüfsumme oder durch eine qualifizierte elektronische Signatur gesichert. Diese integritätssichernden Maßnahmen werden direkt nach dem Eingang der Nachrichten bei dem Diensteanbieter angebracht und an den Empfänger mit übermittelt." Durch die Prüfsummen lassen sich also versendete und erhaltene Dokumente elektronisch vergleichen, ohne, dass man den Inhalt kennen muss. Abweichende Prüfsummen heißt dann: Das versendete und das empfangene Dokument sind nicht vollständig identisch. Wo genau die Unterschiede liegen, muss anschließend aber manuell geprüft werden.



De-Mails sind auf ihrem Weg durch das Internet geschützt
Foto: Bundesamt für Sicherheit in der Informationstechnik

So ist es via De-Mail möglich, offene Dokumentenformate zu versenden, die man mit dem Ursprungsprogramm nachträglich verändern könnte. Das geht zum Beispiel mit allen Word- oder Excel-Dokumenten (die sich allerdings auch gegen Änderungen schützen lassen), nicht aber mit entsprechend codierten PDF-Dateien.

Um die Integrität der über sie verschickten Dokumente zusätzlich sicherzustellen, können die De-Mail-Provider so genannte Dokumentensafes anbieten. Eine Verpflichtung gibt das De-Mail-Gesetz dafür aber nicht vor. In den "De-Safes" können die Kunden versandte und empfangene Dokumente ablegen. "Vertraulichkeit, Integrität und ständige Verfügbarkeit der abgelegten Dokumente sind zu gewährleisten", heißt es dazu im Gesetzestext. Bietet ein Dienstleister diesen Service an, muss er die abgelegten Daten verschlüsseln. Auch hier liegen die Dokumente also dann in einer rechtsverbindlichen, integren Form vor.

Mit diesen Sicherheitsmaßnahmen gewährleistet De-Mail den rechtsgültigen Versand von Dokumenten besser, als das herkömmliche Postdienste garantieren können. Nicht nur die Übermittlung, sondern auch der (verschlüsselte) Inhalt sind über technische Verfahren dokumentiert. Das wird mittelfristig auch Auswirkungen auf den Schriftverkehr mit dem deutschen Rechtssystem haben. So hat **Justizministerin Sabine Leutheusser-Schnarrenberger Anfang Dezember 2011**[9] bekanntgegeben, dass ihr Ministerium an einem Gesetzentwurf zur Einführung des elektronischen Rechtsverkehrs und der elektronischen Fallbearbeitung an Gerichten arbeite. Mit dem Gesetz sollen die Voraussetzungen für vollelektronische Arbeitsabläufe in Strafverfahren geschaffen werden, heißt es in einer Pressemitteilung des Ministeriums anlässlich des 6. Nationalen IT-Gipfels.

Links im Artikel:

[1] **https://www.computerwoche.de/schwerpunkt/p/Phishing.html**
[2] **https://www.computerwoche.de/schwerpunkt/s/Spoofing.html**
[3] **https://www.computerwoche.de/security/2501986/**
[4] **https://www.computerwoche.de/software/erp/1868066/index2.html**
[5] **https://www.computerwoche.de/schwerpunkt/e/E-Mail.html**
[6] **https://www.computerwoche.de/subnet/telekom/de-mail/**
[7] **https://www.computerwoche.de/netzwerke/tk-netze/2490541/index8.html**
[8] **https://www.computerwoche.de/netzwerke/web/2501451/index3.html**
[9] **https://www.computerwoche.de/subnet/telekom/de-mail/**
