



Aktueller Begriff

De-Mail

Mit dem am 3. Mai 2011 in Kraft getretenen Gesetz zur Regelung von De-Mail-Diensten (**De-Mail-Gesetz**) wurde ein gesetzlicher Rahmen zur Einrichtung einer Infrastruktur für sichere elektronische Kommunikation geschaffen. Derzeit können De-Mail-Adressen bei den im Vorbereitungsprozess befindlichen Diensteanbietern reserviert werden. Der für die zweite Jahreshälfte 2011 geplante Start des Angebotes verzögert sich für Privatanwender jedoch vermutlich noch bis Anfang 2012.

Im Gegensatz zu herkömmlichen E-Mails sollen De-Mails als verschlüsselte und nachweisbare elektronische Kommunikationsform von sicher identifizierten Kommunikationspartnern auch für den **offiziellen Schriftverkehr** zwischen Bürgerinnen und Bürgern sowie Behörden, Banken, Versicherungen, Ärzten und Unternehmen geeignet sein. Auch Privatpersonen können untereinander per De-Mail kommunizieren, sofern Adressat wie Empfänger über einen De-Mail-Zugang verfügen. Wirtschaft und Verwaltung rechnen durch die mit De-Mail mögliche Optimierung von Unternehmens- und Verwaltungsprozessen sowie geringeren Transaktionskosten mit einem **Einsparpotential** in Milliardenhöhe.

Eine Nachricht, die im Postfach- und Versanddienst über De-Mail verschickt wird, ist gegen eine unbefugte Einsichtnahme sowie gegen Änderungen ihres Inhalts und ihrer „Metadaten“ (z.B. Absenderadresse, Versandzeit etc.) geschützt. Sie wird verschlüsselt über gesicherte Kanäle vom Absender über den Diensteanbieter, und von diesem wiederum – gegebenenfalls über einen anderen Diensteanbieter – verschlüsselt an den Adressaten gesendet (**Punkt-zu-Punkt-Verschlüsselung**). Zwar bedeutet dies, dass die vertraulichen Daten beim Diensteanbieter kurzzeitig unverschlüsselt vorliegen, bevor sie auf Viren überprüft und wiederum verschlüsselt weitergeleitet werden. Jedoch hat dieses Verfahren den Vorteil, dass der Dienst in seiner Basisvariante für die Anwender ohne zusätzliche Installationen am eigenen Computer über einen Web-Browser nutzbar ist. Dies wird als Voraussetzung für die gewünschte Verbreitung des neuen Kommunikationsangebotes in der Fläche angesehen. Für die Übermittlung von besonders vertraulichen Nachrichten ist eine zusätzliche **Ende-zu-Ende-Verschlüsselung** im Rahmen von De-Mail möglich, die jedoch die Installation zusätzlicher Software für die Ver- und Entschlüsselung auf dem Endgerät des Nutzers erfordert.

Eine zentrale Rolle für die Sicherstellung der Zuverlässigkeit des neuen Dienstes kommt den **Diensteanbietern** zu. Sie haben sich bei dem für das **Sicherheits- und Zertifizierungskonzept** von De-Mail zuständigen **Bundesamt für Sicherheit in der Informationstechnik** (BSI) zu akkreditieren. Voraussetzung dafür ist die nachgewiesene Erfüllung vom BSI festgelegter Standards, die nur durch wiederum vom BSI zertifizierte IT-Sicherheitsdienstleister testiert werden können. Auch die in den Prozess eingebundenen Rechenzentren bedürfen einer offiziellen Zertifizierung.

Nr. 32/11 (03. November 2011)

Ausarbeitungen und andere Informationsangebote der Wissenschaftlichen Dienste geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Der Deutsche Bundestag behält sich die Rechte der Veröffentlichung und Verbreitung vor. Beides bedarf der Zustimmung der Leitung der Abteilung W, Platz der Republik 1, 11011 Berlin.

Für die Eröffnung eines De-Mail-Kontos und die Zuweisung einer De-Mail-Adresse ist es notwendig, sich einmalig eindeutig zu identifizieren, z.B. durch die persönliche Vorlage des Personalausweises. Darüber hinaus sichern weitere Anforderungen wie die „Zwei-Faktor-Authentisierung“ (z.B. mit neuem Personalausweis oder Handy-TAN) das Verfahren zusätzlich gegen einen potentiellen Missbrauch ab. Nach erfolgreicher Eröffnung eines De-Mail-Kontos soll die Handhabung des Dienstes durch die Anwender dem normalen E-Mail-Versand ähneln. Neben der einfachen Nachrichtenübermittlung gibt es die folgenden Versandoptionen: „**Persönlich**“ mit einem höheren Anmeldeniveau („Zwei-Faktor-Authentisierung“) für Sender und Empfänger; „**absenderbestätigt**“ mit einer Bestätigung der Identität des Absenders durch dessen De-Mail-Diensteanbieter per qualifizierter elektronischer Signatur; „**Versandbestätigung**“ mit Erzeugung einer solchen durch den Versanddienst des Absenders und „**Ein-gangsbestätigung**“ mit Erzeugung einer solchen vom Postfachdienst des Empfängers an Sender wie Empfänger. Zusätzlich zur Nachrichtenübermittlung dürfen De-Mail-Diensteanbieter zwei zusätzliche kostenpflichtige Dienste anbieten: **De-Safe** bietet eine verschlüsselte Dokumentenablage auf den Rechnern der Diensteanbieter und **De-Ident** bietet natürlichen Personen und Institutionen einen Identitätsbestätigungsdienst. Für Privatpersonen soll die Einrichtung eines De-Mail-Kontos kostenlos sein, über die Versandkosten gibt es derzeit noch keine eindeutigen Angaben der künftigen Diensteanbieter.

Die Eröffnung eines elektronischen Übermittlungsweges für offizielle Behördenkorrespondenz bringt auch neue Fragen im Zusammenhang mit möglicherweise belastenden Bescheiden oder Fristsetzungen mit sich. Grundsätzlich können Bürgerinnen und Bürger nur dann per De-Mail behördlich kontaktiert werden, wenn sie diesem Kommunikationsweg durch die freiwillige Eröffnung eines De-Mail-Zugangs ausdrücklich zugestimmt haben. Wenn sie zugestimmt haben, gilt ein per De-Mail übersandter Bescheid seitens der Behörde erst dann als **förmlich zugestellt**, wenn vom Diensteanbieter des Adressaten eine „**Abholbestätigung**“ erzeugt und an die absendende Behörde übermittelt wurde – was wiederum eine durch zusätzliche Maßnahmen (Zwei-Faktor-Authentisierung) gesicherte Anmeldung des Adressaten an seinem De-Mail-Postfach voraussetzt. Dagegen greift die durch eine Änderung des Verwaltungszustellungsgesetzes (§ 5a VwZG) neu eingeführte **Zustellungsfiktion** für De-Mail-Nachrichten nur in den seltenen Fällen, bei denen die Behörde aufgrund einer Rechtsvorschrift an die elektronische Abwicklung eines Verfahrens gebunden ist und der Empfänger die Abwicklung per De-Mail vorab verlangt hat (womit der Behörde eine papier-basierte Zustellung nicht mehr möglich ist).

Mit der Verabschiedung des De-Mail-Gesetzes im Februar 2011 kam ein Gesetzgebungsvorhaben zum Abschluss, das in ähnlicher Form mit dem Bürgerportalgesetz bereits in der vorherigen Legislaturperiode den Deutschen Bundestag beschäftigt hatte und das in seinen Zielsetzungen in Politik und Wirtschaft sowie bei vielen gesellschaftlichen Gruppen weitgehend Zustimmung findet. Zu den **Kritikpunkten** an dem nun umgesetzten Konzept zählen jedoch die nicht zwingend vorgesehene Ende-zu-Ende-Verschlüsselung und die gegenwärtig nicht vorhandene Portabilität der De-Mail-Adressen für Privatpersonen bei einem Wechsel des Diensteanbieters.

Derzeit befinden sich mehrere **Diensteanbieter** für De-Mail im Zertifizierungsprozess des BSI. Neben der Deutschen Telekom, United Internet und Mentana Claimsoft zählt dazu auch die Deutsche Post, die mit ihrem Angebot e-post bereits seit Mitte 2010 über ein sehr ähnlich strukturiertes Angebot verfügt. Alle Anbieter gemeinsam verzeichnen derzeit etwa zwei Millionen Voranmeldungen für De-Mail.

Literatur/Quellen:

- Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften. (BGBl I 2011 Nr. 19, 2.5.2011, S. 666.)
- De-Mail – eine Infrastruktur für sichere Kommunikation.
www.bsi.bund.de/ContentBSI/Themen/Egovernment/DeMail/DeMail.html.
- Informationen des IT-Beauftragten der Bundesregierung unter: www.de-mail.de (beide Links zuletzt abgerufen: 29.9.2011).
- Lechtenböcker, Jens. Zur Sicherheit von De-Mail. In: Datenschutz und Sicherheit 4/2011, S. 268 - 269.