

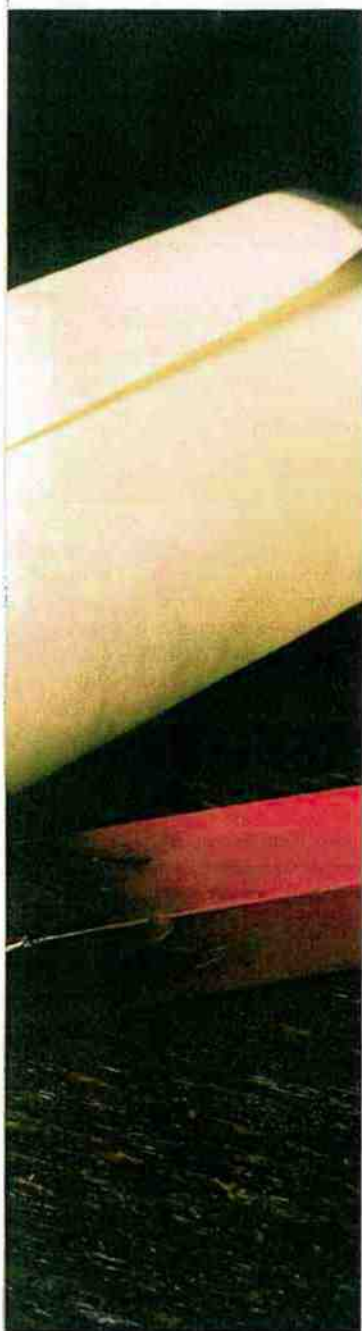
> IT-STRATEGIEN De-Mail



Mit Brief und Siegel

Nach jahrelangen Vorbereitungen steht **das Projekt De-Mail**, das einen rechtssicheren digitalen Nachrichtenversand ermöglicht, unmittelbar vor der Einführung. Der Dienst soll die Kommunikation von Bürgern und Unternehmen mit Behörden erleichtern, doch sein tatsächlicher Nutzen ist (noch) zweifelhaft.

Dr. Carsten Ritterskamp



Oftmals sind Behörden und Unternehmen in der schriftlichen Kommunikation – aus Gründen der Rechtssicherheit – auf den postalischen Versand ihrer Nachrichten angewiesen. Im Vergleich zum elektronischen Versand – etwa per E-Mail – verursacht diese papiergebundene Kommunikation höhere Kosten und macht komplexere Verarbeitungsschritte erforderlich.

Mit De-Mail will der Gesetzgeber öffentliche und private Anwender in die Lage versetzen, die Vorteile der elektronischen Kommunikation auf einem zur Briefpost vergleichbaren Niveau der Rechtssicherheit zu nutzen: Durch das am 3. Mai 2011 in Kraft getretene De-Mail-Gesetz wurden die dafür erforderlichen Rahmenbedingungen geschaffen. Eine Reihe zugehöriger technischer Richtlinien legt die Anforderungen an die IT-Sicherheit der Dienste verbindlich fest.

Konkurrierende Anbieter

Derzeit streben United Internet, Mentana-Claimssoft, die Deutsche Telekom sowie die Deutsche Post AG mit ihrem bereits als eigenständiges System gestarteten E-Postbrief die zur Teilnahme am De-Mail-Netzwerk erforderliche Akkreditierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) an – mit der Markteinführung zertifizierter Angebote ist noch im Lauf dieses Jahres zu rechnen.

In der Praxis stehen Behörden und Unternehmen nun vor der Herausforderung, den Nutzen von De-Mail für sich abzuschätzen und die Möglichkeiten des Zusammenspiels des Verfahrens mit ihren etablierten Abläufen und Systemen zu überprüfen. Denn auch wenn durch das De-Mail-Gesetz ein rechtlicher Rahmen für das verbindliche und vertrauliche Versenden von Dokumenten und Nachrichten über das Internet gegeben wurde: Der elektronische Versandweg steht längst nicht für alle Schriftstücke einer Organisation offen. In welchem Umfang eine Behörde oder ein Unternehmen von De-Mail profitieren kann, hängt von individuell zu überprüfenden organisatorischen, technischen und rechtlichen Rahmenbedingungen ab.

Technische Anbindung

Im Gegensatz zu privaten Endanwendern, die zur Nutzung von De-Mail auf eine Browser-basierende Web-An-

wendung festgelegt sind, können Unternehmen und Behörden De-Mail an ihre bestehende E-Mail-Infrastruktur anbinden.

Da das Nachrichtenformat von De-Mail auf der Spezifikation einer E-Mail gemäß RFC 2822 beruht und erforderliche Erweiterungen ausschließlich über standardkonforme X-Header vorgenommen werden, ist eine solche Integration aus technischer Perspektive nicht übermäßig komplex: Durch ein Gateway werden E-Mails aus der eigenen Organisation als De-Mails aufbereitet und eingehende De-Mails in E-Mails umgewandelt. Zusatzfunktionen zur Verarbeitung De-Mail-spezifischer Sicherheitsmerkmale lassen sich in diversen Mail-Clients durch Plugins nachrüsten.

De-Mails werden zwischen Gateway und Provider und innerhalb des De-Mail-Netzwerks grundsätzlich auf gesicherten Kanälen übertragen. Eine die Vertraulichkeit gewährleistende durchgängige Verschlüsselung der Nachrichten erfolgt aber nur optional und erfordert den zusätzlichen Einsatz eines Public-Key-Verfahrens, wodurch zusätzlicher Aufwand entsteht.

Vor dem praktischen Einsatz von De-Mail ist deshalb zu überprüfen, ob das Sicherheitsniveau einer End-to-End-Verschlüsselung benötigt wird oder ob das De-Mail-Sicherheitskonzept bereits ein hinreichendes Maß an Vertraulichkeit bietet.

Rechtliche Rahmenbedingungen

De-Mail wird stets auf freiwilliger Basis genutzt: Deshalb ist grundsätzlich kein Bürger zur Teilnahme an dem Dienst verpflichtet. Auch wenn er über ein De-Mail-Konto verfügt, ist er unter der zugehörigen Adresse noch nicht für jede Behörde oder jedes Unternehmen erreichbar.

Damit ein Bürger Nachrichten und Dokumente auf rechtsverbindlichem Weg per De-Mail von einer Behörde oder einem Unternehmen erhalten kann, muss er vorab ausdrücklich zugestimmt haben, mit der fraglichen Organisation mittels De-Mail elektronisch kommunizieren zu wollen. Im Unterschied zur klassischen Briefpost verfügt der Bürger bei De-Mail also über sehr weitreichende Möglichkeiten zu bestimmen, für wen er erreichbar sein möchte und für wen nicht.

In der Praxis folgt aus der Notwendigkeit dieser freiwilligen Zugangsöff-

IT-STRATEGIEN De-Mail

> De-Mails allein ersetzen nicht die persönliche Unterschrift. Ob sich der Dienst durchsetzen kann, ist daher fraglich.

sign@ture:

nung, dass vor allem solche Nachrichten zum Versand per De-Mail geeignet sind, deren Erhalt im Interesse des Empfängers liegt. Angesichts dieser Ausgangslage müssen Behörden und Unternehmen revisions sichere Prozesse der Zugangsöffnung etablieren und Anreize dafür schaffen, mit ihnen per De-Mail zu kommunizieren.

Kein Ersatz für die Unterschrift

Zu beachten ist, dass der Kommunikationskanal stets in beide Richtungen geöffnet wird. Eine Organisation, die De-Mails versenden möchte, muss für ihre Kunden auch per De-Mail erreichbar sein.

Beim Versand von De-Mails ist darüber hinaus zu beachten, dass durch das De-Mail-Gesetz vor allem die Anforderungen an einen rechtssicheren elektronischen Versandweg geklärt werden. Formerfordernisse, denen eine Nachricht unter bestimmten Umständen genügen muss, bleiben davon weitestgehend unberührt.

In der Praxis ergeben sich daraus insbesondere dann Einschränkungen, wenn die zu versendende Nachricht der Schriftform bedarf. Der Versand per De-Mail reicht dafür nicht aus. Gemäß Signaturgesetz ist dazu nach wie vor die bei Privatpersonen kaum verbreitete qualifizierte elektronische Signatur erforderlich.

So funktioniert der De-Mail-Versand

Der Postfach- und Versanddienst ist der zentrale Dienst von De-Mail. Er gewährleistet eine zuverlässige und vertrauliche Kommunikation: Eine Nachricht ist beim Versand gegen den Verlust der Vertraulichkeit, gegen Änderungen des Nachrichteninhaltes und der sogenannten Metadaten (zum Beispiel Absenderadresse, Versandzeit und Versandoptionen) geschützt.

Zusätzlich können De-Mails qualifiziert versendet werden. Dabei gibt es vier Versandoptionen:

- ❑ **Persönlich:** Die Wahl dieser Option bedeutet, dass das erforderliche Anmeldeniveau des Empfängers mindestens „hoch“ sein muss, um die Nachricht lesen zu können. Um diese Option wählen zu können, muss auch das Anmeldeniveau des Absenders „hoch“ sein.
- ❑ **Absenderbestätigt:** Mit der Wahl dieser Option bringt der Absender zum Ausdruck, dass er sich verbindlich an den von ihm versendeten Nachrichteninhalte gebunden fühlt. Um diese Option wählen zu können, muss das Anmeldeniveau des Absenders „hoch“ sein. Der Empfänger erfährt, dass der Absender beim Versand der Nachricht „hoch“ angemeldet war.

❑ **Versandbestätigung:** Bei der Wahl dieser Option wird eine Versandbestätigung vom Versanddienst des Absenders erzeugt und dem Absender per Nachricht zugestellt.

❑ **Eingangsbestätigung:** Bei der Wahl dieser Option wird eine Zugangsbestätigung vom Postfachdienst des Empfängers erzeugt und dem Absender sowie dem Empfänger der ursprünglichen Nachricht per Nachricht zugestellt.

Diese vier Optionen kann der Nutzer in beliebiger Kombination wählen. Das Anmeldeniveau „hoch“ erfordert eine Zwei-Faktor-Authentifizierung, zum Beispiel per SMS-TAN. Bei der Anmeldung in der Stufe „normal“ reicht dagegen die Eingabe von Benutzername und Passwort – damit stehen aber nicht alle Versandoptionen zur Verfügung.

Darüber hinaus kann der Absender seine Nachrichten zusätzlich mit seinen eigenen Komponenten (qualifiziert elektronisch) signieren und/oder „Ende zu Ende“ verschlüsseln. De-Mail-Anbieter sind verpflichtet, einen Verzeichnisdienst anzubieten, in dem De-Mail-Nutzer öffentliche Schlüssel/Verschlüsselungs-Zertifikate zu ihren De-Mail-Adressen hinterlegen können. So wird die Möglichkeit der End-to-End-Verschlüsselung für den Nutzer erheblich vereinfacht. [Quelle: BSI]

Gerade für die rechtsverbindliche Kommunikation mit einem Unternehmen oder einer Behörde bietet der vermeintlich sichere und nachweisbare Versand einer De-Mail dem Bürger somit keinen deutlich erkennbaren Mehrwert. Mit einem deutlichen Anstieg der Akzeptanz und der Teilnehmerzahlen ist deshalb erst dann zu rechnen, wenn die De-Mail flächendeckend im Sinne einer „E-Mail mit Unterschrift“ eingesetzt werden kann. Zwar beabsichtigt der Gesetzgeber, das Verhältnis des De-Mail-Gesetzes zum Signaturgesetz zu überprüfen und die De-Mail unter bestimmten Bedingungen als Alternative zur qualifizierten elektronischen Signatur zuzulassen – eine rechtsverbindliche Entscheidung über solche Möglichkeiten steht jedoch noch aus.

Fazit

Auch wenn die Technologien zum Versand elektronischer Nachrichten als De-Mail vergleichsweise einfach in die Systemlandschaft einer Organisation zu integrieren sind: Wirtschaftliche Vorteile sind nicht per se garantiert. Behör-

den und Unternehmen sollten vor dem Hintergrund ihrer individuellen Anforderungen und Rahmenbedingungen sorgfältig überprüfen, in welchem Umfang sie von De-Mail-Kommunikation profitieren können.

Dabei sind gerade auch die Kosten zur Modifikation bestehender Kommunikationsprozesse zu berücksichtigen und in Relation zum erwarteten Rückgang der Versandkosten zu setzen. Denn signifikante Einspar-Effekte können oftmals nur durch einen breitenwirksamen Einsatz des Verfahrens erzielt werden.

Für den erfolgreichen Einsatz von De-Mails ist somit vor allem ein zahlenmäßig großer Nutzerkreis notwendig. Doch dieser wird durch die erforderliche Zugangseröffnung und die aus Sicht des Bürgers oftmals nicht klar erkennbaren Vorteile des Verfahrens beschränkt.

Der Erfolg von De-Mail hängt damit gerade auch davon ab, inwiefern es dem Gesetzgeber, Behörden und Unternehmen gelingen wird, Nutzungsanreize zu schaffen und überzeugende Argumente zur Teilnahme an De-Mail zu kommunizieren. [rm]

DER AUTOR



Dr. Carsten Ritterskamp ■
Senior Consultant bei der adesso AG in Dortmund. Im Mittelpunkt seiner Tätigkeit steht die Beratung zu IT-unterstützten kooperativen Prozessen.