



Das Magazin für Führungskräfte in Kirchen  
und kirchlichen Organisationen

www.kviid.de

## KVI im DIALOG

3 | August 2011

### Finanzen

Werden die ermäßigten Umsatzsteuersätze abgeschafft? Auswirkungen des Grünbuchs der Europäischen Kommission auf die Kirchen und auf die Sozialwirtschaft

### Organisation

Streiten verbindet - Mediation als Chance für eine neue Streitkultur in Kirche und Diakonie

### Energie und Umwelt

Energieeffizienz in kirchlichen Einrichtungen - Literaturhinweise, Klimaneutralität, Energiemanagement, Teil 10

### Personalmanagement

Einsatz mit Gewinn?! Ehrenamt in der stationären Altenhilfe. Chancen - Grenzen - Herausforderungen, Teil 1

### Kirchliche Tagungshäuser

Kloster Hegne feiert Hotelgeburtstag - Fünf Jahre Tagungs- und Urlaubshotel Haus St. Elisabeth am westlichen Bodensee

### Reportage

Gospelkirchentag in Karlsruhe - Umweltmanagement auf dem 5. Gospelkirchentag



**Special:**

**6. KVI Kongress 2011  
Nachbericht**

**Nachbericht**  
6. KVI Kongress 2011  
Ab Seite 19

## Das Ende der Briefpost

Ein Beitrag von Lothar Leger

Die E-Mail ist heute als Kommunikationsmedium nicht mehr weg zu denken. Kaum eine öffentliche oder privatwirtschaftliche Institution, die nicht unter der Last der ein- und ausgehenden e-Mails stöhnt.

Dennoch hat das Verfahren einige signifikante Schwächen. So ist es weit entfernt von einer vertraulichen und sicheren Kommunikation und ihm fehlt damit die rechtliche Anerkennung. Dies soll jetzt mit De-Mail geändert werden. Mit in Kraft treten des „Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften“ im April 2011 setzte die deutsche Bundesregierung eine EU-Richtlinie von 2006 in nationales Recht um<sup>1</sup>. Jeder Bürger und jede Bürgerin, aber genauso auch alle juristischen Personen sollen in absehbarer Zukunft über den zentralen Dienst De-Mail zuverlässig, verbindlich und vertraulich kommunizieren können. Die Sicherheit der Kommunikation des sogenannten Postfach- und Versanddienstes von De-Mail basiert dabei auf der zweifelsfreien Authentifizierung der Kommunikationspartner und einer verschlüsselten Übertragung der Nachricht. In einem Feldversuch in Friedrichshafen konnten Bürgerinnen, Bürger und Organisationen dieses neue Verfahren bereits in 2009 ausführlich testen. Aktuell gibt es viele positive Stimmen, aber auch mindestens genauso viele, die mahnen den Finger heben.

### Verfahren

Der große Nachteil der heutigen E-Mail-Systeme ist, dass sie viele Angriffspunkte für Verfälschungen, Ausspähen und Missbrauch bieten. Zustellungen über das Internet und über E-Mail-Provider sind alles andere als sicher und nachvollziehbar.



Abb.: Deutsche Post AG

Auch die Deutsche Post AG, die in 2010 den e-Post-Dienst auf den Markt gebracht hat, beabsichtigt eine Akkreditierung für De-Mail

Mit De-Mail wird ein Verfahren aufgebaut, das dem einer geschlossenen Benutzergruppe entspricht. Alle Beteiligten sind zweifelsfrei bekannt und können jederzeit identifiziert werden. Jeder, der an De-Mail teilnehmen möchte, muss sich ein entsprechendes Benutzerkonto besorgen. Dazu ist es notwendig, dass er/sie sich einmalig zuverlässig registrieren lässt. Für natürlich Personen werden die persönlichen Daten, wie Vor- und Zuname, Meldeadresse und Geburtsdatum aufgenommen. Das Registrierungsverfahren über den elektronischen Personalausweis oder über das schon von der elektronischen Signatur her bekannte Post-Ident-Verfahren ist ausreichend sicher. Selbstverständlich können sich auch juristische Personen für De-Mail anmelden. Das Verfahren ist identisch. Zusätzlich zu den Basisangaben zu der juristischen Person werden dann zum Beispiel auch Daten der vertretungsberechtigten Personen registriert.

Eine wichtige Rolle in dem Verfahren kommt den Diensteanbietern zu. Sie sind verantwortlich für die Bereitstellung der Dienste und für die zuverlässige und einwandfreie Abwicklung der Kommunikation. Um dem gerecht zu werden, müssen sich interessierte Unternehmen einem Akkreditierungsverfahren unterziehen, das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) durchgeführt wird. Bisher haben sich United Internet AG (GMX.de und WEB.de), Mentana Claimsoft AG, Deutsche Telekom AG, und T-Systems GmbH der Akkreditierung gestellt.

Die Deutsche Post AG, die mit dem e-Post-Dienst ein Konkurrenz-Verfahren auf den Markt gebracht hat, beabsichtigt eine Akkreditierung für De-Mail.

### Angebot

Das Angebot für juristische Personen umfasst den Postfach- und Versanddienst (De-Mail und De-

Mail-Einschreiben), einen Dienst für den Identitätsnachweis (Identitätsbestätigungsdienst oder De-Ident) und einen Dienst zur sicheren Aufbewahrung von Nachrichten (Speicherplatz, Dokumentensafe oder De-Safe). Die Teilnahme ist in jedem Fall und für alle Seiten freiwillig. Zumindest in der Theorie.

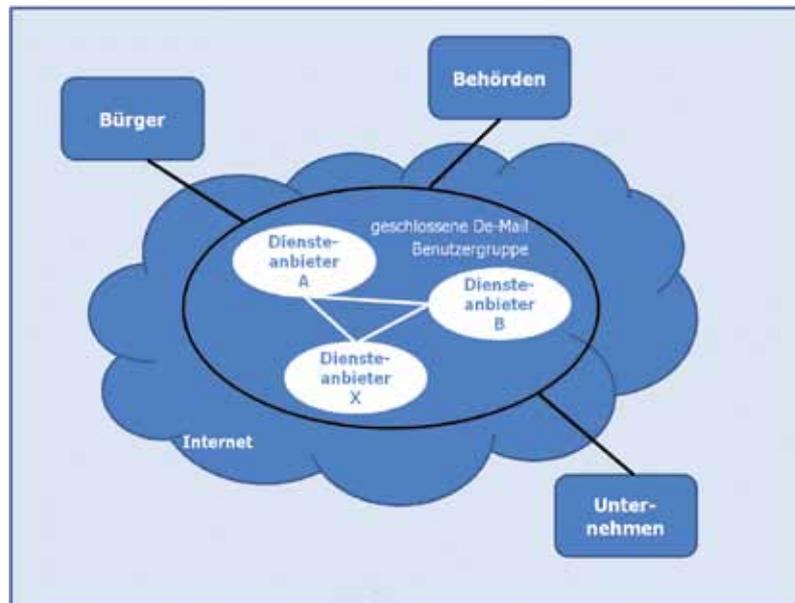
De-Mail sorgt für einen verlustfreien, verbindlichen und vertraulichen Versand. Beim Versand können, ähnlich wie man es auch von bisherigen Mail-Verfahren gewohnt ist, Nachrichten als persönlich/vertraulich eingestuft werden. Darüber hinaus lässt sich einstellen, ob Bestätigungen für das Absenden, die Zustellung und die Abholung gewünscht sind.

Bei De-Mail-Einschreiben erhält der Absender qualifiziert signierte Bestätigung über Datum und Uhrzeit des Versands und des Eingangs beim Empfänger.

Mit De-Ident soll eine jederzeitige Identitätsfeststellung ermöglicht werden. Der De-Mail-Dienstanbieter erstellt auf Anforderung, zum Beispiel im Rahmen einer Registrierung für einen Online-Dienst eine Bestätigung der Identität und übermittelt diese, versehen mit einer qualifizierten elektronischen Signatur an den Anforderer.

Wer für eine sichere Aufbewahrung von De-Mails sorgen will oder muss und wer dafür nicht unbedingt selbst die Infrastruktur aufbauen möchte, kann De-Safe nutzen. Die Dienstanbieter sollen entsprechende Speicherbereiche zur Verfügung stellen, in denen die Nachrichten sicher, verschlüsselt und vor unbefugtem Zugriff geschützt aufbewahrt werden.

Ganz kostenlos werden die Dienste natürlich nicht sein. Die Wirtschaftlichkeitsbetrachtungen setzen vor allem darauf, dass sich die Nutzung



Kommunikationsprinzip De-Mail

von De-Mail über die Einsparung von Porto rechnet. Endgültige Preise für die Nutzung stehen noch nicht fest. Allerdings wird davon ausgegangen, dass die De-Mail-Nachricht deutlich günstiger als das Porto für einen Brief ist. Dies ist übrigens einer der wesentlichen Unterschiede zum Konkurrenz-Produkt e-Post. Hier liegen die Preise zwar auch unterhalb der üblichen Portogebühren, aber eben nicht signifikant. Leider sind die tatsächlichen Gebühren- und Preisstrukturen noch unbekannt und es kann nur mit Annahmen gearbeitet werden.

### Auswirkungen

Nach dem Willen der Bundesregierung, respektive der zuständigen Ministerien, soll mit De-Mail ein neuer und sicherer Kommunikationsweg entstehen. Für öffentliche Einrichtungen und Unternehmen bedeutet dies, dass sie nicht umhin kommen, sich mit dem Verfahren auseinanderzusetzen. Auch wenn eine Teilnahme für alle Beteiligten freiwillig ist, so kann es doch zu einem gewissen Druck durch Bürger oder Geschäftspartner kommen, wenn diese De-Mail nutzen möchten. Fakt ist, dass mit De-Mail

Briefporto und Druckkosten nachhaltig eingespart werden können. Das sollte Grund genug sein, mindestens ein Evaluierungsprojekt aufzusetzen.

Allerdings ist es mit der Auswahl des Diensteanbieters und der Einrichtung einer De-Mail-Adresse nicht getan. Auch die interne Organisation muss entsprechend angepasst werden. Neben informationstechnischen Fragen (u.a. Form der Anbindung, Schnittstelle zwischen dem bisherigen E-Mail-System und De-Mail-Gateways, zusätzliche Verschlüsselung) sind vor allem organisatorische Fragen zu klären. So ist zu definieren, wie die neuen und zusätzlichen De-Mail-Adressen in die bestehende Mail-Adressen-Logik zusammengeführt werden können. Auf jeden Fall muss nachvollziehbar bleiben, welche Nachrichten per herkömmlicher E-Mail und welche Nachrichten mit De-Mail verschickt / empfangen wurden. Darüber hinaus ist zu klären, wo empfangene und gesendete De-Mail-Nachrichten archiviert werden. Mit De-Safe wird zwar eine sichere Aufbewahrung angeboten, allerdings liegen die Dokumente dann beim Diensteanbieter

und sind damit, entsprechende Verdachtsmomente vorausgesetzt, in einem sehr leichten Zugriff für alle relevanten Behörden.

Besonders wichtig ist darauf zu achten, dass eine an sich verbindliche und rechtssichere De-Mail-Nachricht sehr schnell ihre Beweiskraft verlieren kann, wenn sie die geschlossene Benutzergruppe verlässt (zum Beispiel bei interner Weiterleitung per E-Mail). Auch das Thema Ende-zu-Ende-Verschlüsselung ist noch nicht hinreichend geklärt. De-Mail sorgt nur von dem Gateway beim Absender bis zum Gateway beim Empfänger für Vertraulichkeit und Verschlüsselung.

In den zuständigen Behörden geht man davon aus, dass sich die Anzahl der über Bürgerportale versendeten Nachrichten langsam aber stetig über die nächsten Jahre entwickeln wird und dass bis 2015 rund 20% der grundsätzlich in Frage kommenden Nachrichten tatsächlich über Bürgerportale (also via De-Mail) versendet werden. Auf absehbare Zeit werden sich Unternehmen und Organisationen somit auf einen zusätzlichen Kommunikationskanal einstellen müssen, der neben den bisherigen (Briefpost, E-Mail, Fax und Telefon) zu berücksichtigen ist.

### Herangehensweise

Die neue Entwicklung einfach zu ignorieren, wäre sicher die schlechteste aller Alternativen. Deshalb ist es besser, in einem ersten Schritt auszuloten, was eine Einführung und Nutzung von De-Mail für die eigene Organisation bedeutet. Dies kann zum Beispiel in Form einer überschaubaren Machbarkeitsstudie geschehen. Als Ergebnis sollten die technischen Anforderungen, absehbare organisatorische Veränderungen und eine Kosten- Nutzen-Betrachtung erwartet werden. Dabei ist

auch die Variante „keine Nutzung von De-Mail“ zu betrachten. Als erstes sind die heute ausgehenden Briefe und E-Mails darauf zu untersuchen, ob überhaupt Bedarf für mehr Rechtsverbindlichkeit und Sicherheit besteht.

Bei der Wirtschaftlichkeitsbetrachtung sollten mehrere Szenarien mit unterschiedlichen Annahmen zu den Preisen gerechnet werden. Es empfiehlt sich, hier auch einmal die Alternative e-Post als weitere Alternative einzubeziehen. Zu empfehlen ist auch eine Differenzierung in der Betrachtung nach Gruppen von Kommunikationspartnern. Dies könnte unter anderem zeigen, dass eine stufenweise Einführung angebracht ist oder dass für einige Gruppen De-Mail nicht opportun ist. Voraussetzung ist in jedem Fall eine kritische Masse von Nachrichten, bei denen rechtsverbindliche Briefe notwendig sind.

Zu guter Letzt ist zu klären, wie und wo empfangene und gesendete De-Mail-Nachrichten abgelegt und aufbewahrt werden und wie sie den Arbeitsvorgängen zugeordnet werden können. Aus den vorangegangenen Arbeiten kann dann eine individuelle Strategie abgeleitet werden, die es umzusetzen gilt.

### Ausblick

Die rechtliche Situation ist seit Veröffentlichung des De-Mail-Gesetzes im Bundesgesetzblatt am 2. Mai 2011 geregelt. Allerdings sind die Preismodelle der verschiedenen Dienstleister noch nicht endgültig definiert. Eine Klärung soll im Laufe des Jahres 2011 erfolgen. Ob sich De-Mail wirklich so schnell entwickelt, wie es in Publikationen immer wieder beschrieben wird, ist abzuwarten. Auch bei der elektronischen Signatur glaubte man an einen raschen Siegeszug, der an vielen Stellen an der Akzeptanz scheiterte.

De-Mail hat viel Potenzial. Wir alle wünschen uns einen einfachen und dennoch sicheren, zuverlässigen und verbindlichen Austausch von Briefen und Nachrichten. Die Bürgerportale und De-Mail sind dabei genau der richtige Ansatz. Entscheidend für die Akzeptanz ist, dass das Verfahren einfach und für jeden nachvollziehbar bleibt und dass dem einzelnen, sei er natürlich oder juristische Person, keine Nachteile entstehen. Bis dahin haben die Verantwortlichen noch einiges zu tun. Die Ablösung und damit das Ende der Briefpost wird also noch länger auf sich warten lassen.



Dipl.-Wirtsch.-Ing. Lothar Leger, Geschäftsführer der B&L Management Consulting GmbH und Kenner des DMS/ECM Marktes