



So einfach wie E-Mail und so sicher wie die Papierpost

E-Mails sind unsicherer als die Papierpost und werden daher für viele Geschäftsvorfälle nicht eingesetzt.

E-Mails können ohne großen Aufwand auf ihrem Weg durch das Internet abgefangen, wie Postkarten mitgelesen und in ihrem Inhalt verändert werden. Absender und Empfänger können nie vollständig sicher sein, mit wem sie gerade kommunizieren und ob die gesendete E-Mail tatsächlich beim Empfänger angekommen ist. Der Anteil von SPAM (also unerwünschten, massenhaft versendeten E-Mails eines zumeist nur schwer oder gar nicht ermittelbaren Absenders) am E-Mail-Verkehr hat stark zugenommen. Auch das Ausspähen von Zugangsdaten zu E-Mail-Konten („Phishing“, Identitätsdiebstahl) wird immer häufiger.

Dies alles hat bislang den Durchbruch von E-Mails überall dort verhindert, wo es auf Vertraulichkeit (verschlüsselt), Verlässlichkeit (angekommen) und Verbindlichkeit (eindeutige Identität) ankommt, die zusammen wichtige Voraussetzungen für die Gewährleistung von Rechtsicherheit sind.

Am Markt existierende Lösungen haben sich nicht in der Fläche durchsetzen können, da diese häufig zusätzliche Installationen auf den Rechnern der Nutzer erfordern (Zertifikate, Kartenlesegerät, etc.). Weniger als fünf Prozent des gesamten E-Mail-Aufkommens sind heute verschlüsselt.

De-Mail ermöglicht Vertraulichkeit, Verlässlichkeit und Verbindlichkeit in der elektronischen Kommunikation.

Als Weiterentwicklung der „einfachen“ E-Mail bietet De-Mail eine einfach zu nutzende Technologie, mit der man sicher im Internet miteinander Nachrichten austauschen kann. Ein wichtiges Ziel von De-Mail ist dabei, grundlegende Sicherheitsfunktionen bezogen auf Vertraulichkeit, Verlässlichkeit und Verbindlichkeit für den Austausch elektronischer Nachrichten einfach nutzbar (d.h. ohne zusätzliche Installationen beim Nutzer) und dadurch möglichst breit verfügbar zu machen.

Versender und Empfänger einer De-Mail sind nachvollziehbar. Versand- und Zustellnachweise können einfach erstellt werden (Einschreiben). De-Mails sind auf dem Transport verschlüsselt und können daher nicht von Dritten abgefangen und/oder verändert werden. SPAM wird wirksam verhindert, weil Absender von De-Mails über eine sichere Erstidentifizierung eindeutig bekannt sind. Phishing und Identitätsdiebstahl können ausgeschlossen werden, wenn sich Nutzer beispielsweise mit dem künftigen elektronischen Personalausweis oder einem Mobiltelefonbasierten Verfahren (mobile TAN) bei De-Mail anmelden.

Durch diese zusätzlichen Sicherheitsfunktionen kann ein großer Teil der bislang noch auf Papier abgewickelten Geschäfts- und Verwaltungsprozesse mit De-Mail einfacher, schneller und von jedem Ort aus vollständig elektronisch erledigt werden.

De-Mail ist dabei in der Handhabung so einfach wie die E-Mail.

Die Bedienung von De-Mail durch Bürger und Unternehmen erfolgt im einfachsten Fall durch Web-Anwendungen, die in der Handhabung den bekannten Angeboten von E-Mail-Providern sehr ähnlich sind und beim Nutzer keine weiteren Installationen von Hardware oder Software erfordern. Unternehmen und Behörden können ihre existierenden (internen) E-Mail-Infrastrukturen über ein



So einfach wie E-Mail und so sicher wie die Papierpost

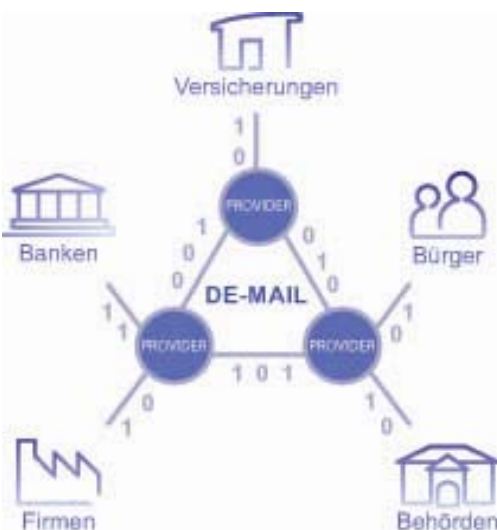
sog. „Gateway“ an De-Mail anschließen, so dass ihre Mitarbeiterinnen und Mitarbeiter die vorhandenen E-Mail-Clients weiterverwenden können.

De-Mail-Konten können sowohl von Bürgerinnen und Bürgern als auch von Unternehmen oder der Verwaltung eröffnet werden. Für die Eröffnung müssen sich die Nutzer einmal zuverlässig identifizieren (z.B. über Post-Ident-Verfahren oder den elektronischen Personalausweis). Die regelmäßige Anmeldung zur Nutzung von De-Mail kann über Nutzernamen/Passwort, über den elektronischen Personalausweis, Mobiltelefonbasierte Verfahren (mTAN) oder andere sichere Verfahren erfolgen.

De-Mail ist damit so einfach wie die E-Mail und so sicher wie die Papierpost.

Staat und Wirtschaft definieren gemeinsam den Rahmen. Die Wirtschaft setzt De-Mail um.

Lediglich die Rahmenbedingungen für den sicheren Nachrichtenaustausch im Internet über De-Mail müssen vom Staat geschaffen werden. Die Umsetzung von De-Mail in Form konkreter Produkte bzw. Dienste erfolgt durch interessierte Unternehmen, die sich an diesen Rahmen halten.



Die grundlegenden Anforderungen an Sicherheit, Funktionalität und Interoperabilität wurden vom Bund gemeinsam mit den künftigen De-Mail-Providern erarbeitet und in Form von technischen Richtlinien festgeschrieben. Die Einhaltung dieser Richtlinien durch De-Mail-Provider wird in einem gesetzlich geregelten Akkreditierungs- und Zertifizierungsverfahren geprüft.

Das Angebot von De-Mail-Diensten erfolgt so durch miteinander im Wettbewerb stehende Unternehmen, die sich auf Grundlage des einheitlichen Rahmens durch Zusatzangebote voneinander abgrenzen können. De-Mail ist damit die Basis für eine flächendeckende und gleichzeitig wettbewerbsfreundliche Infrastruktur für sichere elektronische Kommunikation.

De-Mail berücksichtigt Anforderungen des Datenschutzes und ermöglicht Selbst-Datenschutz und Datensicherheit.

Die gesetzlichen Regelungen zu De-Mail sehen vor, dass die Provider im Rahmen des Akkreditierungsverfahrens neben den oben erwähnten Zertifikaten für Sicherheit, Funktionalität und Interoperabilität auch umfassende Maßnahmen zum Schutz der personenbezogenen Daten belegen müssen. Für diesen gesetzlich geforderten Datenschutznachweis wurden geeignete Kriterien erarbeitet und abgestimmt.

Mit besonderem Blick auf den Datenschutz schreibt das De-Mail-Konzept u.a. vor, dass De-Mail-Provider zum Schutz vor Rückverfolgbarkeit in Kommunikations- oder Konsumentenprofilen das Einrichten von pseudonymen E-Mail-Adressen vorsehen müssen. Weiterhin müssen die De-Mail-Provider auf Wunsch die Verschlüsselungszertifikate der Nutzerinnen und Nutzer im Verzeichnis vorhalten, um die (zusätzliche) Ende-zu-Ende-Verschlüsselung von De-Mails zu unterstützen.



So einfach wie E-Mail und so sicher wie die Papierpost

De-Mail ist daneben aufgrund der obligatorischen Verschlüsselung der übermittelten Daten für die Nutzer ein wichtiges Instrument zur Verbesserung des Selbst Datenschutzes und der Datensicherheit.

Regelmäßige Prüfungen in technisch-organisatorischer Hinsicht und gesetzlich vorgeschriebene Sicherheitsmaßnahmen im Rahmen der Zertifizierung/Akkreditierung sorgen dafür, dass die Provider Datenschutz und Datensicherheit für die Nutzer und ihre persönlichen Daten auf hohem Niveau gewährleisten.

Im Ergebnis können Sicherheit und Vertraulichkeit beim Austausch elektronischer Nachrichten mit De-Mail von einem heute flächendeckend geringen Niveau auf ein flächendeckend hohes Niveau angehoben werden.

Ein großer Teil der Anwendungsfälle von De-Mail betrifft die elektronische Kommunikation in den Bereichen B2B und B2C.

De-Mail ist keine „Behörden-Mail“, wie zum Teil berichtet wird, sondern eine Infrastruktur für den sicheren Austausch elektronischer Nachrichten, die sich vor allem auch an Bürgerinnen und Bürger sowie Unternehmen richtet. Die Verwaltung ist eine weitere Nutzergruppe.

Beispiele für Anwendungsfelder von De-Mail in der Wirtschaft sind für die Kommunikation

- mit Geschäftspartnern: Vertragsangebote, Abnahmeerklärungen, Auftragsbestätigungen, Kostenvoranschläge usw.
- mit Mitarbeitern: Gehaltsmitteilungen, Personalangelegenheiten usw.
- mit Behörden: Antragsverfahren, regelmäßige Meldungen usw.
- mit Kammern und Verbänden: regelmäßige Meldungen, Anträge usw.

Allein bei den deutschen Versicherern, die jährlich rund 800 Millionen Schreiben per Briefpost versenden, sind laut Gesamtverband der Versicherungswirtschaft (GDV) so Einsparungen von mehreren hundert Millionen Euro pro Jahr möglich. Daher wird De-Mail aktiv vom Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) unterstützt. Das gleiche gilt für den Hightech-Verband BITKOM sowie den eco – Verband der deutschen Internetwirtschaft.

Wirtschaft und Verbände unterstützen De-Mail bei der Pilotierung in Friedrichshafen.

Mit den ersten De-Mail-Providern GMX, T-Home, T-Systems und WEB.DE wurde De-Mail inzwischen so weit fertiggestellt, dass die Pilotierung am 9. Oktober 2009 in der Stadt Friedrichshafen am Bodensee begonnen wurde (www.fn.de-mail.de). An den Tests beteiligen sich u.a. die Firmen AWD, Citibank, CosmosDirekt, EADS, Gothaer, HUK24, LVM, Sparkasse Bodensee, Volksbank Friedrichshafen, ZF sowie die Stadt Friedrichshafen, die Handwerkskammer Ulm und die IHK Bodensee/Oberschwaben - und viele Bürgerinnen und Bürger, die De-Mail während der Pilotierung kostenlos nutzen können.



So einfach wie E-Mail und so sicher wie die Papierpost



Foto: BITKOM versendet die erste De-Mail an Prof. Zorn. Quelle: BMI/Hans-Joachim M. Rickel

Als Startschuss der Pilotierung wurde die erste De-Mail durch den BITKOM an Herrn Prof. Zorn verschickt, der als einer der Gründungsväter des deutschen Internet vor 25 Jahren auch die erste E-Mail in Deutschland erhielt.. (www.bmi.bund.de/Pressemitteilung).

Ziel der Pilotierung – die auf sechs Monate festgelegt ist – ist insbesondere die Erhebung der Nutzerakzeptanz von De-Mail in unterschiedlichen Anwendungsfeldern zwischen Unternehmen und Bürgern sowie mit und innerhalb der Verwaltung.

Auftretende Akzeptanzprobleme und Schwierigkeiten in der Bedienung sollen früh erkannt

und behoben werden, sodass mit Beginn des Wirkbetriebes allen Bürgerinnen und Bürgern, Unternehmen und Behörden eine ausgereifte und anerkannte Plattform zur Verfügung gestellt werden kann.

De-Mail ist voraussichtlich in der zweiten Jahreshälfte 2010 verfügbar.

Die Zulassungskriterien für De-Mail-Provider werden durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht. Rechtliche Voraussetzung für die Zulassung ist ein Gesetz. Es konnte als Bürgerportal-Gesetz in der letzten Wahlperiode vom Bundestag aus Zeitgründen nicht mehr verabschiedet werden. CDU und FDP haben die Verabschiedung eines De-Mail-Gesetzes in ihre Koalitionsvereinbarung aufgenommen. Vor diesem Hintergrund ist geplant, dass De-Mail in der zweiten Jahreshälfte 2010 zur Verfügung steht.

Weitere De-Mail-Provider sind willkommen.

Mehr als ein Jahrzehnt nach dem „Internet-Boom“ ist in Deutschland immer noch keine flächendeckende Infrastruktur für den vertraulichen und rechtssicheren Austausch von elektronischen Nachrichten verfügbar.

Die umfassende Unterstützung des De-Mail-Projekts durch Internet-Services-Provider (wie GMX, T-Home, T-Systems, WEB.DE, etc.), den BITKOM sowie durch Unternehmen gibt inzwischen deutliche Hinweise darauf, dass der jetzt erarbeitete staatliche Rahmen für De-Mail künftig einen funktionierenden Markt ermöglicht, durch den weitere Insel-Lösungen vermieden werden können.

Das De-Mail-Projekt wirkt daher fortlaufend auf eine Beteiligung weiterer Unternehmen am künftigen Verbund von De-Mail-Providern hin.