Warum ein E-Government-Gesetz?

Es ist ein Gebot der Bürgernähe, dass staatliche Verwaltungen Bürgerinnen und Bürger für Behördenkontakte im privaten, ehrenamtlichen und wirtschaftlichen Alltag Online-Dienste ermöglichen und erleichtern. Es handelt sich dabei um ein Angebot zur orts- und zeitunabhängigen Kommunikation. Transaktionen verlangen sehr oft die Schriftform, d. h. ein unterschriebenes Blatt Papier. Diese kann bislang nur durch die qualifizierte elektronische Signatur ersetzt werden, die keine Verbreitung gefunden hat. Für die Anwender war sie nicht nutzerfreundlich genug. Deshalb blieb es de facto dabei, dass Bürgerinnen und Bürger mit der Verwaltung per Papier mit Unterschrift verkehren. Wie eine neuere Statistik von Eurostat zeigt, suchen zwar 51 % der Deutschen elektronisch Kontakt mit den Behörden, aber nur 15 % der ausgefüllten Formulare werden elektronisch an die Behörden zurückgeschickt, weil nur so das Schriftformerfordernis erfüllt werden kann. Damit liegt Deutschland in der EU auf Rang 20 (hinter Griechenland, Malta, Slowakei und weit hinter den großen Staaten)[1].

Was soll geregelt werden?

Mit dem Gesetz wird geregelt, dass außer der qeS zwei weitere, nutzerfreundliche Verfahren künftig im Verkehr mit Behörden die Unterschrift ersetzen können. Die beiden Verfahren sind: Erstens die spezielle E-Mail-Variante „De-Mail“, bei der beide Kommunikationspartner sicher identifiziert sind, und zweitens Webanwendungen der Verwaltung in Verbindung mit der elektronischen Identifikationsfunktion des neuen Personalausweises. Damit sollen für die „elektronische Unterschrift“ Verfahren zur Verfügung stehen, die die Funktionen der Unterschrift zuverlässig erfüllen können und auch für IT-Laien einfach anwendbar sind.

Warum diese Technologien?

Beide Verfahren sind einfach und ohne großen technischen Aufwand zu bedienen und genügen zugleich den Sicherheitserfordernissen.

Wie wird bei De-Mail die Vertraulichkeit sichergestellt?

Bei der Konzeption von De-Mail wurde eine Verschlüsselung aller versendeten Nachrichten durch den De-Mail-Provider vorgesehen, um die Vertraulichkeit zu schützen. So ist jede übermittelte De-Mail auf ihrem Weg durch das Internet verschlüsselt. Die De-Mail-Provider müssen im Rahmen der Akkreditierung nachweisen, dass sie genau definierte Anforderungen an die technische und organisatorische Sicherheit erfüllen.

Optional kann jede Bürgerin und jeder Bürger entscheiden, beim Versender der De-Mail und beim Empfänger der De-Mail zusätzliche Software zur Verschlüsselung zu nutzen.

Was heißt das für mich als Bürger?

De-Mail ist eine einfache und sehr sichere Kommunikationsmethode.

---

[1] Aktuelle Statistik (19.03.2013) Eurostat - Kommunikation mit Behörden/ Einzelpersonen: http://epp.eurostat.ec.europa.eu/portal/page/portal/product_details/dataset?p_product_code=ISOC_BDEK_PS

Die Nutzung von De-Mail ist für Unternehmen und Privatpersonen freiwillig. Wer von einer Behörde eine De-Mail erhalten möchte, muss der Behörde zunächst mitteilen, dass sie oder er zukünftig auf diesem Weg erreichbar sein möchte.

Wer lieber Papier versenden oder persönlich bei der Behörde vorsprechen möchte, kann das auch in Zukunft tun.

Das E-Government-Gesetz bietet eine zusätzliche Option für Bürger und Unternehmen im Kontakt mit der Verwaltung: eine einfache und sichere elektronische Kommunikation. Der Bürger hat die Wahl.

Was wird kritisiert?

Kritisiert wird, dass die Verschlüsselung bei De-Mail nicht sicher genug sei, gefordert wird eine zusätzliche sogenannte „Ende-zu-Ende-Verschlüsselung".

Dies wird insbesondere für den Versand von Sozial- und Steuerdaten per De-Mail thematisiert, weil dies häufig sensible Daten sind.

Warum wurde Ende-zu-Ende-Verschlüsselung bei De-Mail nicht als Regelfall vorgeschrieben, sondern kommt nur optional zum Einsatz?

Nach Schätzungen sind heute weniger als 5% der E-Mails verschlüsselt, obwohl E-Mails beim Transport durch das Internet leicht abgefangen und mitgelesen werden können. Grund für die geringe Zahl der verschlüsselten E-Mails ist zum einen das noch nicht ausreichend ausgeprägte Sicherheitsbewusstsein. Zum anderen ist die Verschlüsselung für den Endkunden schwer realisierbar.

Wollte man eine zusätzliche Ende-zu-Ende-Verschlüsselung bei De-Mail verpflichtend einsetzen, würde man die Einfachheit des De-Mail-Dienstes opfern. Im Regelfall müsste der Nutzer eine zusätzliche Software installieren und wissen, wie man diese bedient. Außerdem müsste der Sender einer Nachricht mit dem Empfänger Schlüsselinformationen austauschen. Insbesondere das Versenden von E-Mails aus dem Browser – das die meisten Nutzer heute (mit weiter steigender Tendenz) verwenden - würde hierdurch erheblich komplizierter.

Ein weiteres Problem wäre die Aufbewahrung des privaten Schlüssels. Wenn der private Schlüssel des Nutzers verloren ginge (z.B. durch versehentliches Löschen oder einen Hardwaredefekt), hätte er danach keinen Zugriff auf die bereits erhaltenen Nachrichten mehr.

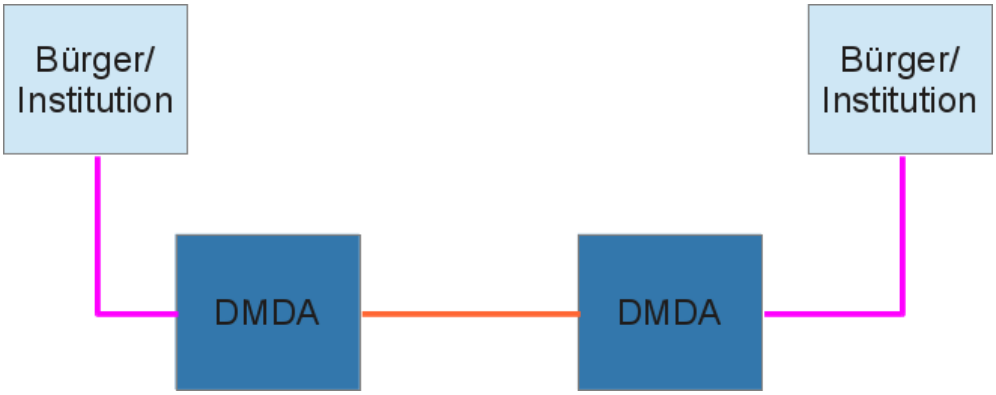
Die geschilderten Probleme im Hinblick auf Ende-zu-Ende-Verschlüsselung würden sich weiter potenzieren, wenn Nutzer mehrere unterschiedliche Endgeräte zum Abruf ihrer De-Mails benutzen möchten, da in diesem Fall auf allen diesen Endgeräten Software installiert und Schlüssel verwaltet werden müssten.

De-Mail stellt grundlegende Sicherheitsfunktionen wie die Verschlüsselung daher beim Provider sicher zur Verfügung. Mit dem De-Mail-Gesetz wurden die entsprechenden Vorgaben definiert. Vier Unternehmen haben derzeit De-Mail im Angebot.

Wie funktioniert die Verschlüsselung bei De-Mail?

De-Mail nimmt dem Nutzer den Aufwand der Verschlüsselung ab und bietet für jede De-Mail eine automatische Verschlüsselung auf dem Transport . Diese Transportverschlüsselung funktioniert folgendermaßen:

In Abbildung 1 sind dazu die Beteiligten und der Kommunikationsweg abgebildet. DMDA steht für den Provider, den „De-Mail-Diensteanbieter“.



1. Zwischen dem Nutzer (Bürger oder Institution) und dem DMDA wird eine verschlüsselte Verbindung aufgebaut (ähnlich wie z.B. auch beim Online-Banking).
   Danach identifiziert sich der Nutzer gegenüber seinem DMDA (meldet sich also mit Benutzername und Passwort und ggf. einem weiteren Sicherungsmittel wie z. B. der eID-Funktion des nPA an).

2. Die Nachricht wird über den verschlüsselten Kommunikationskanal zum Server des Providers übertragen. Mitlesen im Internet ist nicht mehr möglich. Auf dem Server des Providers wird die Nachricht automatisiert (also ohne dass ein Mitarbeiter des DMDA konkret handelt) bearbeitet (z.B. Überprüfung auf Schadsoftware, Hinzufügen von Metadaten wie Datum, Uhrzeit, usw.)

3. Der DMDA baut eine verschlüsselte Verbindung zum DMDA des Empfängers auf und überträgt die Nachricht. Auf dem Server des Providers des Empfängers wird ebenfalls vollautomatisiert die Nachricht in verschlüsselter Form im Postfach des Empfängers abgelegt.

4. Der Empfänger baut eine verschlüsselte Verbindung zu seinem DMDA auf, identifiziert sich und ruft die Nachricht ab.

Damit ist die De-Mail beim Transport im Internet immer verschlüsselt und auch während der Lagerung der Nachricht im Postfach des Absenders bzw. des Empfängers.

Wie werden die Nachrichten bei der Verarbeitung durch den Mailprovider geschützt?

Das De-Mail-Gesetz und die Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) schreiben zahlreiche organisatorische und technische Sicherheitsmaßnahmen vor, damit es auf den Servern der Provider nicht zum Einblick in die De-Mail-Nachrichten kommen kann:

- Die IT-Systeme sind speziell gegen Angriffe gehärtet (durch Entfernung/Deaktivierung nicht genutzter Funktionen des Betriebsystems , Abschottung durch Firewalls, regelmäßige Updates, Virenscanner, Überwachung der Systemeigenschaften und -anwendungen)

- Das Dateisystem ist verschlüsselt, so dass bei einem Diebstahl der Datenträger kein Zugriff darauf möglich ist. Es ist daher auch kein direkter Zugriff auf Backup-Daten möglich.

- Die Nachrichten werden in verschlüsselter Form in den Postfächern abgelegt. Zur sicheren Aufbewahrung des Schlüssels kommen spezielle Hardwarekomponenten, sogenannte Hardware Security Modules (HSM) zum Einsatz. Der Schlüssel kann auf diese Weise nicht entwendet werden.

- Der DMDA muss durch sein Rollenkonzept nachweisen, dass die Aufgaben für die Schlüsselverwaltung und der Verwaltung der Daten durch unterschiedliche Administratoren erfolgen.

- Der Zugriff auf einen Server oder Daten in Postfächern erfordert daher, dass zwei Administratoren gemeinsam handeln.

- Alle Aktivitäten der Administratoren auf den einzelnen IT-Systemen werden aufgezeichnet. So ist nachvollziehbar, welche Person was getan hat. Die Logdaten müssen regelmäßig ausgewertet werden. Dabei ist der Logdatenadministrator nicht identisch mit den anderen beiden Administratoren.

- Alle Administratoren, die beim DMDA hinsichtlich De-Mail zum Einsatz kommen, müssen im Rahmen der Akkreditierung nach De-Mail-G ein polizeiliches Führungszeugnis vorlegen.

Die Umsetzung der Maßnahmen wurde im Rahmen der Akkreditierung nach De-Mail-G geprüft. Nur die Provider, die alle Maßnahmen umgesetzt haben, wurden vom BSI zugelassen.

Hierbei wurde ein weltweit einzigartiges hohes Schutzniveau bei der Verschlüsselung elektronischer Nachrichten durch E-Mail-Provider erreicht. Drei unterschiedliche Mitarbeiter eines akkreditierten und überprüften Providers müssten mit hoher krimineller Energie zusammenwirken, um De-Mails beim Provider mitzulesen. Die hierfür aufzubringende kriminelle Energie und das technische Know-How sind weit höher als etwa beim heimlichen Öffnen von Briefen durch Postmitarbeiter nötig wären.

Verwaltungsvorgänge mit besonders hohen Sicherheitsanforderungen

Der Entwurf des E-Government-Gesetzes regelt allein den Schriftformersatz. Damit geht diese Regelung nicht spezifischen Datenschutz-, Geheimschutz oder anderen Fachregelungen vor. Das bedeutet, dass im Einzelfall zu prüfen ist, ob nicht ein besonders gesicherter Übertragungsweg gewählt werden muss. Für wenige Fälle besonders sensibler Daten kann ausnahmsweise nur eine Ende-zu-Ende-Verschlüsselung ein geeignetes Verfahren sein – z.B. wenn „die Schadensauswirkungen bei unberechtigtem Zugriff ein existentiell bedrohliches Ausmaß erreichen“,

während bei normalen Verwaltungsdaten auch nach Auffassung des BfDI De-Mail ohne zusätzliche Ende-zu-Ende-Verschlüsselung ausreicht[2].

Es wäre schwierig, hierzu eine allgemeine Regelung zu formulieren: Die Daten, bei denen eine Ende-zu-Ende-Verschlüsselung ausnahmsweise notwendig ist, können nicht abschließend umschrieben werden. So gibt es keine geeignete gesetzliche Definition von beispielsweise in diesem Zusammenhang besonders relevanten „Sozialdaten“ oder „Gesundheitsdaten“, an die man anknüpfen könnte. Die Legaldefinition des Begriffs „Sozialdaten“ in § 67 SGB X („Sozialdaten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden.“) ist so allgemein gefasst, dass darunter auch Daten wie z.B. Name, Anschrift, Geburtsdatum fallen. Dies sind Daten, die normalerweise in den Schutzbedarf „normal“ fallen (vgl. für das Datum „Anschrift“ die Handreichung des BfDI vom 1. März 2013, S. 6; www.bfdi.bund.de). Wie sich aus der Handreichung des BfDI weiter ergibt, ist die Beurteilung aber kontextabhängig und erfordert in jedem Einzelfall eine vorhergehende Risikoanalyse. So ist der Schutzbedarf des Datums „Anschrift“ dann als „sehr hoch“ einzustufen, wenn sich die betreffende Person in einem Zeugenschutzprogramm befindet.

Wäre es sinnvoll, De-Mails generell Ende-zu-Ende zu verschlüsseln?

Nein, denn der Vorteil der Nutzerfreundlichkeit wäre dann dahin. Die Masse aller E-Mail-Nutzer würden De-Mail wegen des dann damit verbundenen technischen Aufwandes nicht nutzen. De-Mail wäre keine Massen-Anwendung für Bürgerinnen und Bürger mehr, sondern eine Nischen-Anwendung für Spezialisten.

---

2 http://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/DEMail/DeMailHandreichung.pdf?__blob=publicationFile S. 6.