TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der IT-Sicherheitsverband.

PRESSEMITTEILUNG

TeleTrusT: Qualifizierte Elektronische Signatur und De-Mail sind einander ergänzende Technologien

Kommentierung anlässlich der Beratungen der Gesetzentwürfe zur Förderung des elektronischen Rechtsverkehrs

Berlin, 25.03.2013 – Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) kommentiert insbesondere anlässlich der Position von Bündnis 90/Die Grünen in der jüngsten Bundestagsdebatte zu den Gesetzentwürfen zur Förderung des elektronischen Rechtsverkehrs der Verwendungszweck von Qualifizierter Elektronischer Signatur und De-Mail. Beides sind einander ergänzende, aber nicht gleichzusetzende Technologien.

Im Zuge der Beratungen der Gesetzentwürfe zur Förderung des elektronischen Rechtsverkehrs in der Justiz bzw. mit den Gerichten vertritt Bündnis 90/Die Grünen die Position, dass die "die im Regierungsentwurf in § 130 a Abs. 4 Nr. 1 ZPO als 'sicherer Übermittlungsweg' markierte De-Mail keineswegs so sicher wie eine qualifizierte elektronische Signatur" sei. TeleTrusT kommentiert hierzu:

Die Sichtweise der Fraktion BÜNDNIS 90/Die Grünen vertieft ein im Gesetzentwurf des FördElRV angelegtes Missverständnis, nämlich die Vermengung bzw. Gleichstellung der qualifizierten elektronischen Signatur (QES) und des sog. "sicheren Übermittlungswegs", insbesondere in Form der De-Mail, als wären dies Alternativen zueinander. Die QES ist jedoch weder eine Technologie zur Übermittlung von Nachrichten noch bewirkt sie die Verschlüsselung und damit die Vertraulichkeit der signierten Daten. Die QES sichert vielmehr wie kein anderes Mittel die Authentizität und die Integrität des signierten Dokuments (also seine rechtssichere Zuordnung zum Urheber und seine Unverfälschtheit) und gewährleistet damit die Rechtssicherheit im elektronischen Rechtsverkehr.

Zur elektronischen Kommunikation mit der Justiz wird – in Kombination mit der QES – bereits seit vielen Jahren das Elektronische Gerichts- und Verwaltungspostfach (EGVP) verwendet, das über eine Ende-zu-Ende-Verschlüsselung verfügt und damit die Vertraulichkeit bestmöglich sichert. Auch De-Mail bietet bereits eine höhere Vertraulichkeit als eine herkömmliche E-Mail und kann optional mit Ende-zu-Ende-Verschlüsselung betrieben werden, um dann den gleichen Vertraulichkeitsschutz wie das EGVP zu erlangen. Zu Recht will der Gesetzentwurf auf die QES des Einreichers nur bei der sog. absenderbestätigten De-Mail verzichten, die gegenüber der einfachen De-Mail mit einer QES des De-Mail-Providers geschützt ist und somit einen erhöhten Authentizitäts- und Integritätsschutz bietet. Die QES erfüllt lediglich eine Formvorschrift, schützt jedoch nicht vor Datenmissbrauch. Die QES ist nur in Deutschland einsetzbar, weil eine EU-weite Regelung zur Rechtsverbindlichkeit fehlt.

§ 130 a ZPO regelt, welche Form elektronische Dokumente haben sollen. Vertraulichkeit und Datenschutz sind Themen, die die Art der Zustellung betreffen. De-Mail ist in der Tat nicht geeignet, den bisherigen Normzweck zu erfüllen – der Gesetzentwurf fügt nur eine Regelung zur Art des Transports hinzu, der derzeit in § 130 a ZPO gar nicht geregelt ist. §130 a ZPO überträgt die Anforderung "Schriftform" für elektronische Dokumente in das Gesetz. Die Schriftform ist eine Eigenschaft, die dem Dokument hinzugefügt wird. Dafür eignet sich eine Signatur.

De-Mail hingegen hat Berechtigung als Transportweg, ist aber nicht geeignet, dauerhaft und unabhängig von De-Mail archivierbar die Eigenschaft eines Dokuments zu ändern bzw. zu sichern. De-Mail ermöglicht erstmals, dass es ein digitales Äquivalent zum physischen Brief gibt. Somit existiert nun für viele kommunale, öffentliche und privatwirtschaftliche Versender ein sicherer digitaler Kanal. Die QES sichert hingegen ein Dokument und verleiht der Unterschrift/Signatur Beweiskraft. Dies gilt unverändert und soll auch so bleiben. In der Fläche ist das aber kein probates Mittel, da beim Bürger im Zweifelsfall keine Signatur-

Infrastruktur vorhanden ist. Hier kann De-Mail helfen. Bei Verwendung einer absenderbestätigten De-Mail erbringt der DMDA des Versenders eine QES für den Versender, wenn dieser sich vorab hoch-authentisiert hat, etwa mittels nPA. Der Versender ist damit hinreichend sicher authentisiert und der Empfänger erhält eine qualifiziert signierte De-Mail, die ggf. auch Anlagen/Dokumente beinhaltet. Die QES fehlt bei De-Mail also nicht, sondern ergänzt sie in sinnvoller Art und Weise.

TeleTrusT – Bundesverband IT-Sicherheit e.V., Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 /40054310, holger.muehlbauer@teletrust.de
www.teletrust.de