

ZENTRALER KREDITAUSSCHUSS

MITGLIEDER: BUNDESVERBAND DER DEUTSCHEN VOLKSBANKEN UND RAIFFEISENBANKEN E.V. BERLIN · BUNDESVERBAND DEUTSCHER BANKEN E.V. BERLIN
BUNDESVERBAND ÖFFENTLICHER BANKEN DEUTSCHLANDS E.V. BERLIN · DEUTSCHER SPARKASSEN- UND GIROVERBAND E.V. BERLIN-BONN
VERBAND DEUTSCHER PFANDBRIEFBANKEN E.V. BERLIN

Stellungnahme des Zentralen Kreditausschusses zum Entwurf des Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften - De-Mail-Gesetz

23. Juli 2010

Mit der angestrebten Einführung von De-Mail-Diensten wird ein wichtiger Beitrag zur Sicherheit und Rechtsverbindlichkeit der Kommunikation zwischen Bürgerinnen, Bürgern, Wirtschaft und Verwaltung im Internet geleistet. Es wird die Möglichkeit geschaffen, vertrauliches Handeln über das Internet zu festigen und zu stärken. Damit tatsächlich der angestrebte Nutzen erreicht wird, sollten die folgenden Punkte aus Sicht der deutschen Kreditwirtschaft im weiteren Gesetzgebungsverfahren berücksichtigt werden:

zu § 3 Abs. 2 Prüfung Identifizierungsdaten

"(5) Dem akkreditierten Diensteanbieter [...]. Er hat sicherzustellen, dass die jeweiligen Nachweise und Informationen in angemessenem zeitlichen Abstand auf ihre Aktualität überprüft werden."

Aus diesem Punkt ist nicht eindeutig erkennbar, ob der Diensteanbieter somit verpflichtet ist, Änderungen der Anschrift seiner Kunden aktiv nachzuvollziehen. Eine Konkretisierung an dieser Stelle halten wir für notwendig.

In B Besonderer Teil zu § 3 sollte nicht nur die Identifizierung nach dem Geldwäschegesetz sondern auch die im Signaturgesetz genannten Anforderungen an die Identifizierung erwähnt werden. Auch sollte der antragstellenden Person ermöglicht werden, sich durch ein qualifiziertes Zertifikat ausweisen zu können. Gegebenenfalls müssten hierfür die nicht im Zertifikat enthaltenen Identifizierungsdaten wie beispielsweise die Adresse von der antragstellenden Person mittels qualifizierter elektronischer Signatur bestätigt werden

zu § 4 sichere Anmeldung an einem De-Mail-Konto Absatz 1

§ 4 „Sichere Anmeldung an einem De-Mail-Konto“ fordert eine sichere Anmeldung mit einem hierfür geeigneten Verfahren. Ein geeignetes Verfahren setzt dabei „[...] zwei voneinander unabhängige Sicherungsmittel.“ voraus. Der Begriff „Sicherungsmittel“ ist in diesem Kontext nicht definiert. Damit ist nicht genau nachvollziehbar, was "zwei voneinander unabhängige Sicherungsmittel“ sein können und ob die Kombination PIN und PIN damit möglich wäre. Eine Präzisierung halten wir für notwendig.

Wir weisen zudem darauf hin, dass bei De-Mail-Diensten auch Transaktionen durchgeführt werden. Einliefern und Abholen sind nach Stand der Technik transaktionsgebundene Verfahren,

bei denen zur Absicherung Methoden wie beispielsweise Signatur oder TAN-Generator einzusetzen sind. Die alleinige Nutzung der elektronischen Identitätsfunktion des neuen Personalausweises ist hierfür nicht ausreichend.

Die Aussage "Die Anmeldung an ein De-Mail-Konto erfolgt auf Verlangen des Nutzers nur als sichere Anmeldung" ist unserer Auffassung nach zu ungenau. Dies impliziert, dass der Nutzer das sichere Verfahren abwählen kann. Jedoch sind bisher keine Kriterien für die Sicherheit des Verfahrens beschrieben. Diese liegt im Verantwortungsbereich des Diensteanbieters. Eine Konkretisierung ist hier notwendig.

zu § 4 Abs. 2 in Zusammenhang mit B Besonderer Teil

In § 4 Absatz 2 wird festgelegt, dass der elektronische Identitätsnachweis nach §18 PAuswG als Verfahren für die sichere Anmeldung unterstützt werden muss. Nach den zugehörigen Anmerkungen in B. Besonderer Teil soll hierdurch ein Anscheinsbeweis für die Authentizität der Handlung entstehen.

Hier sollte deutlich gemacht werden, dass dies nur im Zusammenhang mit einem Cat-S Leser mit eigenem Display, authentischer Anzeige des Diensteanbieters auf dem Leserdisplay und ausschließlicher Eingabe der PIN über die Lesertastatur gilt. Bei Nutzung eines CAT-B Lesers kann nicht von einem Verfahren für eine sichere Anmeldung ausgegangen werden.

Der Diensteanbieter sollte verpflichtet werden, den Nutzer hierüber vor der erstmaligen Nutzung im Rahmen seiner Aufklärungs- und Informationspflichten (gemäß Abschnitt 3, §9) geeignet zu informieren.

Zudem wird hierzu in B Besonderer Teil erläutert, dass zur besseren Nutzbarkeit auch eine Anmeldung mit Nutzernamen und Passwort möglich sei. In diesem Falle sollte der Diensteanbieter verpflichtet werden, den Nutzer darauf hinzuweisen, dass bei Anmeldung mit Nutzernamen und Passwort der Anscheinsbeweis anfechtbar ist und eine rechtsverbindliche Zustellung nicht gewährleistet ist

Bereits in der Stellungnahme vom Dezember 2008 hatte wir folgende Aussage getätigt: „In der Begründung (jetzt B Besonderer Teil) zu § 4, Absatz 2 wird angeführt, dass die Beweissicherheit der Bestätigung etwa durch eine qualifizierte elektronische Signatur des akkreditierten Diensteanbieters über die Bestätigung gewährleistet werden kann. An dieser Stelle sollte ergänzt werden, dass auch ein elektronisches Siegel, das dem Vernehmen nach in das Signaturgesetz aufgenommen werden soll, ebenso die Beweissicherheit der Bestätigung gewährleisten kann, wenn die Akkreditierung des Diensteanbieters die Sicherheit des Verfahrens bestätigt hat.“

Hierzu möchten wir ergänzen, dass bei der sicheren Zustellung (z. B. Einschreiben) die Absicherung auch mit einem "elektronischen Firmenstempel" möglich sein sollte. Dem Bundesministerium für Wirtschaft (BMWi) wird ein Referentenentwurf zur Änderung des Signaturgesetzes, dem Vernehmen nach, noch bis Ende Juli/August 2010 vorgelegt werden.

zu § 5 Abs. 1-2 Postfach / URL

Die Eindeutigkeit dieses neuen Kommunikationskanals wird mit der Randnotiz in Frage gestellt. Eine Uneindeutigkeit an dieser Stelle erschwert die technische Handhabung und mindert die Außenwahrnehmung des Dienstes. De-Mail-Adressen wären dann mit anderen „normalen“ Email-Adressen verwechselbar.

Empfehlung:

Es sollte eine einzige einheitliche Top-Level Domain für den De-Mail Service eingerichtet werden.

zu § 5 Abs. 9 Abholbestätigung

Hier beschreibt der Entwurf, dass eine öffentliche Stelle zur förmlichen Zustellung eine Abholbestätigung verlangen kann. Die Notwendigkeit die Möglichkeit auf eine öffentliche Stelle zu begrenzen, geht nicht aus dem Entwurf hervor, Es bleibt offen, wie eine Abholbestätigung beispielsweise von Einsprüchen durch nicht-öffentliche Stellen, wie Bürger oder Unternehmen bei öffentlichen Stellen sichergestellt ist.

Empfehlung:

Wir regen daher eine Gleichbehandlung von öffentliche und nicht-öffentliche Stellen mit entsprechenden Regelungen an.

zu § 5 Abs. 10 Löschung von Nachrichten

Wir weisen darauf hin, dass mit diesem Punkt die Gefahr verbunden ist, dass ein unbestätigtes Löschen von explizit quittierten Eingängen Missbrauch durch Dritte ermöglicht, die eventuell Zugang zu diesem De-Mail-Konto erlangt haben. Eventuell könnte sogar der Post-Provider die Emails - bei geeigneten AGBs - nach 90 Tagen automatisch löschen (siehe §11).

Empfehlung:

Alle Eingänge sollten daher nur nach sicherer Anmeldung löscher sein.

zu § 5 Abs. 11 Automatische Weiterleitung

Gemäß Absatz (11) kann der Nutzer eine automatische Weiterleitung an eine weitere De-Mail-Adresse einstellen. Wir bitten an dieser Stelle um eine Konkretisierung, ob in diesem Fall eine Zugangsbestätigung (siehe Absatz 8) beziehungsweise eine Abholbestätigung (siehe Absatz 9) nur beim Eingang in das letzte Postfach der Weiterleitungskette ausgestellt wird oder ob alle zwischengeschalteten Postfächer ebenfalls eine Zugangsbestätigung ausstellen.

zu § 10 Sperrung und Auflösung des De-Mail-Kontos

In diesem Paragraphen sind mögliche Gründe für die Sperrung des Zugangs zum De-Mail-Konto genannt. Für den Fall, dass der Kunde sein Authentisierungsmerkmal wie beispielsweise den neuen

Personalausweis bei einem Dritten sperrt, stellt sich die Frage, ob der Zugang des Bürgers zu seinem De-Mail-Konto auf Grund des fehlenden Identitätsnachweises automatisch gesperrt wird oder ob der Bürger den Zugang zusätzlich bei seinen Diensteanbieter sperren lassen muss. Darüber bleibt die Frage offen, ob die Möglichkeit der Zustellung von elektronischen Nachrichten in dem Fall der automatischen Sperre bestehen bleibt oder ob eine Zustellung nicht mehr möglich ist.

zu § 11 Abs. 2 und § 12 Einstellung Diensteanbieterdienst

Sollte ein akkreditierter Diensteanbieter seine Tätigkeit einstellen und kein anderer akkreditierter Diensteanbieter seine Tätigkeit übernehmen, muss dieser sicherstellen, dass die im Postfach und in der Dokumentenablage gespeicherten Daten für wenigstens 3 Monate abrufbar sind.

Empfehlung:

Die Frist erscheint uns zu kurz gefasst und sollte daher auf mindestens 12 Monate ausgedehnt werden. Für den Fall der Einstellung des Betriebes muss das Konto unbedingt von einem anderen Diensteanbieter übernommen werden.

zu § 14 Jugendschutz

Aus dem Paragraphen geht nicht eindeutig hervor, inwieweit sich die Schutzpflichten des Providers auf die Inhalte des Postfaches beziehen. Unklar ist dabei, ob der Provider verpflichtet ist die Inhalte gegebenenfalls zu durchsuchen.

Empfehlung:

Die Inhalte der Nachrichten sollten ausgenommen werden.

zu § 16 Abs. 1 Auskunftsanspruch

Es werden hierbei keine Kriterien genannt, inwieweit der Anbieter die Glaubhaftigkeit eines Anspruchs prüfen muss. Im Zweifelsfall ist der Anbieter dazu nicht ausreichend qualifiziert, was Missbrauchspotenziale öffnet. Die Verfolgung eines beliebigen Rechtsanspruchs sollte vermieden werden.

Empfehlung:

Ein Auskunftsanspruch sollte grundsätzlich nur auf Basis einer gerichtlichen Verfügung bestehen.

zu § 17 Akkreditierung von Diensteanbietern

Die Akkreditierung des Diensteanbieters sollte sich nur auf den De-Mail-Dienst beziehen, nicht auf elektronische Postfächer im Allgemeinen. Die Rechtslage bezüglich der sicheren Zustellung sollte sich bei den herkömmlichen elektronischen Postfächern durch das De-Mail-Verfahren nicht verschärfen.

zu § 18 Voraussetzung der Akkreditierung; Nachweis

Aus dem gegenwärtigen Gesetzentwurf geht nicht eindeutig hervor, dass die Möglichkeit einer Teilakkreditierung besteht. Im entsprechenden Abschnitt ist ausschließlich der Fall beschrieben, dass für Teilleistungen wie beispielsweise den Identitätsdienst eine Akkreditierung zusammen mit einem Anbieter erfolgen muss, der den Pflichtdienst Postfach- und Versanddienst anbietet. Es kann nicht im Sinne des Gesetzes sein, dass sich Provider, die einzelne Teildienste an verschiedene Diensteanbieter offerieren möchten, mehrfach zusammen mit dem jeweiligen Anbieter akkreditieren lassen müssen. Das Angebot von Teilleistungen muss daher separat möglich und akkreditierbar sein.

zu § 22 Standardisierungsgremium

Die Diensteanbieter sollen an der Weiterentwicklung der technischen und organisatorischen Anforderungen beteiligt werden, indem sie an den Sitzungen des Ausschusses De-Mail-Standardisierung teilnehmen können.

Um die Akzeptanz der De-Mail-Dienste unter den Dienstenutzer zu erhöhen, sollten diese ebenfalls in die Weiterentwicklung eingebunden werden.

Die deutsche Kreditwirtschaft kann auf umfangreiche praktische Erfahrungen zum Beispiel im Hinblick auf sichere Identifizierung zurückgreifen und sollte daher, zusammen mit anderen Vertretern der Wirtschaft, frühzeitig in die Entwicklung der Anforderungen an De-Mail-Dienste eingebunden werden.

Erklärung zum Zustellungsgesetz § 5 a

§ 5 a, Absatz 4 erläutert, dass ein elektronisches Dokument als zugestellt gilt, auch wenn der Behörde nach Absendung an das De-Mail-Postfach keine Abholbestätigung innerhalb von drei Tage zugegangen ist. Der Bürger soll in diesem Zusammenhang beweisen, dass ihm eine E-Mail nicht zugegangen ist.

Empfehlung:

Sendungen dürfen erst mit Zustellbestätigung als zugestellt gelten, für entsprechende De-Mails ist eine Empfangsbestätigung notwendig.

Änderung des BGB 312e, Gegenseitigkeitsprinzip für den Einsatz von De-Mail

Versender von De-Mail Nachrichten müssen De-Mail akzeptieren und sollen nicht auf andere Formate verweisen dürfen.

Unformatierte Aufträge sind jedoch für viele Bereiche des Bankgeschäfts nicht akzeptabel.

Es sollte daher aufgenommen werden, dass in speziellen Fällen - wie eben Online-Banking - auf besondere separate Zugangswege / Angebote (und deren Absicherung) verwiesen werden darf.