



Bundesministerium  
des Innern



Freiheit  
Einheit  
Demokratie

POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

An den  
Präsidenten  
des Deutschen Bundestages  
– Parlamentssekretariat –  
Reichstagsgebäude  
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin

POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681-

FAX +49 (0)30 18 681-

INTERNET [www.bmi.bund.de](http://www.bmi.bund.de)

DATUM 22. Dezember 2008

BETREFF **Kleine Anfrage der Abgeordneten Gisela Piltz u. a und der Fraktion der FDP  
Planungen der Bundesregierung zur Einführung von De-Mail  
BT-Drucksache 16/11268**

Auf die Kleine Anfrage übersende ich namens der Bundesregierung die beigegefügte Antwort in  
5-facher Ausfertigung.

In Vertretung

Peter Altmaier

Kleine Anfrage der Abgeordneten Gisela Piltz u. a. und der Fraktion der FDP

Planungen der Bundesregierung zur Einführung von De-Mail

BT-Drucksache 16/11268

---

Antworten:

Zu 1.

Die heute schon vorhandenen Systeme sind technische Lösungen, die sichere elektronische Kommunikation in einem bestimmten Einsatzbereich (z. B. ein Land oder eine Stadt mit ihren Bürgerinnen und Bürgern, im Bereich der Justiz, Wirtschaftsunternehmen mit ihren jeweiligen Kundinnen und Kunden) auf viele verschiedene Weisen und auf verschiedenen Sicherheitsniveaus umsetzen. Die Akzeptanz solcher Systeme bei Bürgerinnen und Bürgern ist entsprechend gering. Einzelne technische Lösungen sind keine Alternative zu einer in Bezug auf Sicherheits-, Datenschutz- und Interoperabilitätsanforderungen einheitlichen Infrastruktur. Die Ausbildung einer Infrastruktur – die „De-Mail“ – ermöglicht die vertrauliche und verbindliche elektronische Kommunikation aller mit allen (Wirtschaft, Bürger, Verwaltung, sonstige Organisationen) auf einem einheitlichen und definierten Sicherheits- und Datenschutzniveau.

Zu 2.

Sichere Verschlüsselungsmethoden gewährleisten lediglich den Schutz der Vertraulichkeit einer Nachricht. Authentizität von Absender und Empfänger sind damit i. d. R. nicht gesichert. Auch lassen sich damit Versand und Zustellung einer Nachricht nur sehr schwer nachweisen. Die verschlüsselten Internet-E-Mails können z. B. auf dem Transportweg gelöscht werden, ohne dass dies bemerkt wird. Die Rechtsverbindlichkeit einer lediglich verschlüsselten E-Mail ist deshalb für zahlreiche Geschäfts- und Verwaltungsprozesse nicht ausreichend.

Die Technologien (z. B. bei Ende-zu-Ende-Verschlüsselung und/oder Signaturen) setzen vielfach voraus, dass der Nutzer selbst die entsprechenden Software-Komponenten installiert, zugehörige Zertifikate für seine Kommunikationspartner verwaltet und geeignet mit den privaten Schlüsseln umgeht. Hier haben die Erfahrungen der vergangenen Jahre gezeigt, dass eine flächendeckende Verbreitung solcher Lösungen nur sehr schwer zu erreichen ist. Bei De-Mail können diese Aufgaben, für die der Nutzer bisher selbst verantwortlich war, von vertrauenswürdigen Anbietern durchgeführt werden. Die privatwirtschaftlichen Anbieter müssen dazu in einem Akkreditierungsverfahren nach-

- 2 -

weisen, dass sie hohe Voraussetzungen an IT-Sicherheit, Datenschutz und Verbraucherschutz erfüllen. Damit kann der Nutzer einen Webbrowser oder einen Standard-E-Mail-Client für sichere Kommunikation verwenden.

Zu 3.

Der elektronische Identitätsnachweis des künftigen elektronischen Personalausweises soll von der De-Mail in zweierlei Hinsicht genutzt werden können. Einerseits soll damit eine Online-Erstidentifizierung und damit die Beantragung eines De-Mail-Accounts möglich sein. Andererseits kann der elektronische Personalausweis zum Anmelden am De-Mail-Account auf einem hohen Sicherheitsniveau verwendet werden.

Zu 4.

Auch mit einer verschlüsselten E-Mail-Kommunikation in Verbindung mit dem elektronischen Personalausweis können Versand und Zustellung von Nachrichten sowie deren Integrität und Verbindlichkeit nur schwer nachgewiesen werden. Im Übrigen wird auf die Antwort zu Frage 1 verwiesen.

Zu 5.

Die bestehenden E-Mail-Adressen von Bürgerinnen und Bürgern bleiben von den Regelungen zu De-Mail völlig unberührt und können wie bisher weiter verwendet werden. Bürgerinnen und Bürger, die an De-Mail teilnehmen möchten, erhalten hierfür eine eigene De-Mail-Adresse, die i. d. R. das Format „vorname.name.123@providerxy.de-mail.de“ hat. Darüber hinaus ist jeder De-Mail-Provider verpflichtet, seinen Kundinnen und Kunden pseudonyme De-Mail-Adressen anzubieten. Diese werden durch einen Zusatz besonders gekennzeichnet - z. B. „ps\_hansi@providerxy.de-mail.de“.

Zu 6.

Ja, sog. pseudonyme Adressen, siehe Antwort zu Frage 5.

Zu 7.

Wie in Antwort zu Frage 5 dargelegt, gibt es keine „den De-Mail-Adressen zugrunde liegenden E-Mail-Adressen“.

- 3 -

Zu 8.

Es gibt keinen automatischen oder verpflichtenden Eintrag von De-Mail-Adressen in ein Melderegister. Die derzeitigen Überlegungen sehen lediglich vor, dass Bürgerinnen und Bürger ihre De-Mail-Adresse freiwillig in ein Melderegister eintragen lassen können.

Zu 9.

Eine ausschließliche Nutzung der De-Mail im Rahmen der EU-Dienstleistungsrichtlinie mit den einheitlichen Ansprechpartnern oder mit Behörden ist nicht geplant.

Zu 10.

entfällt

Zu 11.

Für die Kommunikation mit Behörden ist eine Teilnahme am De-Mail-System nicht verpflichtend. De-Mail ist ein möglicher Kanal für die Kommunikation von Bürgerinnen und Bürgern mit Wirtschaft und Verwaltung, der aufgrund seiner definierten Sicherheit, Einfachheit und Einheitlichkeit die Teilnahme an E-Government-Services erheblich erleichtern wird.

Zu 12.

Die genauen Preise wird jeder Anbieter individuell im Wettbewerb um die Kunden festlegen. Da es auch den De-Mail-Providern darum geht, möglichst viele Kunden zu akquirieren, ist davon auszugehen, dass die Preismodelle auch für Bürgerinnen und Bürger attraktiv sein werden.

Zu 13.

Nein.

Zu 14.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Sicherheitsprofil für mobile Synchronisationsdienste erstellt, welches Sicherheitsanforderungen spezifiziert, um u. a. E-Mails zwischen Behördennetzen und mobilen Endgeräten sicher synchronisieren zu können.

Zu 15.

Auf die Antwort zu Frage 14 wird verwiesen.

Zu 16.

Nein, die Bundesregierung beauftragt keine eigenen Entwicklungen, sondern beschafft gemäß der jeweiligen (Sicherheits-)Anforderungen der Behörden Lösungen am Markt.

Zu 17.

Auf die Antwort zu Frage 16 wird verwiesen.

Zu 18.

Die Möglichkeit, sich akkreditieren zu lassen, steht jedem interessierten Unternehmen offen. Die zukünftigen akkreditierten De-Mail-Provider werden miteinander im Wettbewerb um De-Mail-Kunden stehen. Um beispielsweise die Interoperabilität ihrer Dienste zu sichern, müssen sie auf bestimmten Ebenen zusammen arbeiten.

Zu 19.

Soweit möglich setzt das geplante Zertifizierungsverfahren auf bestehende Verfahren auf und ergänzt sie um dienstspezifische Besonderheiten. Das BSI veröffentlicht in Form Technischer Richtlinien die zu erfüllenden Zertifizierungskriterien hinsichtlich Funktionalität, Interoperabilität und IT-Sicherheit und nimmt in dem Bereich die Zertifizierung vor. Von Bund oder Ländern anerkannte Auditoren überprüfen die Erfüllung dieser Zertifizierungskriterien im Bereich Daten- und Verbraucherschutz. Konnten alle erforderlichen Zertifizierungen vom De-Mail-Provider erfolgreich abgeschlossen werden, wird er auf Antragstellung und Vorlage der erforderlichen Nachweise von der zuständigen Behörde, entsprechend dem Entwurf zum Bürgerportalgesetz das BSI, akkreditiert und kann damit seinen De-Mail-Betrieb aufnehmen. Die Akkreditierung muss regelmäßig erneuert werden.

Zu 20.

Das Zertifizierungsverfahren orientiert sich an den heute üblichen Verfahren für die Sicherheitszertifizierung (z. B. nach Common Criteria oder gemäß ISO 27001 auf Basis von IT-Grundschutz). Die Akkreditierung von De-Mail-Providern obliegt der zuständigen Behörde. Ein eigenes Schlichtungsverfahren ist nicht geplant.

Zu 21.

Bei De-Mail handelt es sich um eine sichere dezentrale Lösung, die von staatlich zertifizierten und akkreditierten Providern aus der Privatwirtschaft bereitgestellt wird. Der Staat schafft einen rechtlichen Rahmen und die regulatorischen Voraussetzungen für eine vertrauenswürdige elektronische Kommunikation für alle. Eine Zertifizierung der einzelnen Dienste und Komponenten der De-Mail-Provider ermöglicht geprüfte statt nur geglaubte Sicherheit, hebt das Sicherheits- und Datenschutzniveau, garantiert die weitgehende Einheitlichkeit der Dienste und fördert die Transparenz. Bürgerinnen und Bürger können deshalb zu Recht Vertrauen in die neue Infrastruktur haben. Zudem haben sie die Möglichkeit, sich einen De-Mail-Provider ihres Vertrauens auszuwählen.

Zu 22.

Akkreditierte De-Mail-Provider können einen zertifizierten virtuellen Dokumentensafe („De-Safe“) anbieten, damit ihre Kundinnen und Kunden De-Mails und andere elektronische Dokumente langfristig, sicher und vertraulich ablegen können. Ein De-Safe ist immer eindeutig einem De-Mail-Konto zugeordnet und gestattet nur Zugriffe durch den Inhaber dieses Kontos.

Zu 23.

Die Konzeption sieht genau diese Variante vor, nämlich Dokumente per De-Mail jeweils an den Empfänger zu versenden und keineswegs auf einem Server (De-Safe) zum Download zur Verfügung zu stellen. Damit dient der De-Safe lediglich der sicheren Ablage eigener Dokumente - ohne Zugriffsmöglichkeiten durch Dritte.

Zu 24.

Die De-Safes befinden sich bei den privaten De-Mail-Providern. Ein staatliches Zertifizierungsverfahren hinsichtlich IT-Sicherheit und Datenschutz gewährleistet geprüfte Sicherheit und Vertraulichkeit und erhöht das Vertrauen in die privaten Provider. Dieses Konzept bietet gute Voraussetzungen für Akzeptanz bei Bürgerinnen und Bürgern.

Zu 25.

In anderen Ländern gibt es - wie in Deutschland auch - eine Reihe von Ansätzen, die sich auf die elektronische Kommunikation bestimmter Zielgruppen beschränken, z. B. zwischen oder mit Behörden bzw. zwischen großen Unternehmen. Ein übergreifender Ansatz wie bei der De-Mail, bei dem es um die elektronische Kommunikation zwischen Bürgerinnen und Bürgern, Wirtschaft und Verwaltung geht, ist nicht bekannt.

Zu 26.

Die üblichen elektronischen Kommunikationswege wie besonders E-Mail sind für die Kommunikation im Rahmen der EU-Dienstleistungsrichtlinie nur bedingt bis gar nicht geeignet. De-Mail bietet für die elektronische Kommunikation mit den einheitlichen Ansprechpartnern im Rahmen der EU-DLR - im Gegensatz zu z. B. normaler E-Mail - erhebliche Vorteile. Ein verpflichtender Einsatz der De-Mail, um aus dem EU-Ausland mit deutschen Behörden elektronisch kommunizieren zu können, wird daraus nicht abgeleitet.

Zu 27.

Länder und Kommunen wurden auf vielfältige Weise einbezogen, durch Veranstaltungen und Treffen mit Vertretern von Ländern und Kommunen, sowie durch den Austausch mit der OSCI-Leitstelle in Bremen, dem Deutschen Städtetag, Vitako, der Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e.V.. Darüber hinaus werden sich die spezifischen kommunalen Anforderungen durch die Pilotierung der De-Mail in der Region Friedrichshafen nachhaltig im Projekt niederschlagen.

Zu 28.

Um an De-Mail teilzunehmen, kann sich eine Behörde/ eine Stadt bei einem Provider einen Account für juristische Personen einrichten, der selbst Unterpostfächer für z. B. verschiedene Abteilungen, Referate oder auch Mitarbeiter enthalten kann. Bei der Behörde ist die Implementierung eines Gateways erforderlich, das in einer einfachen Version als Open Source Software bereitgestellt werden soll. Auf den Arbeitsplatzrechnern der Mitarbeiter ist i. d. R. keine zusätzliche Software nötig, da auf die bestehende E-Mail-Infrastruktur zurückgegriffen werden kann.

Im laufenden Betrieb fallen für die De-Mail nutzenden Behörden voraussichtlich Kosten für den Versand von De-Mails an, ggf. können auch Flat-Rates zwischen Behörde/Stadt/Land und dem Provider vereinbart werden. Die Höhe dieser Kosten wird unter Marktbedingungen zwischen Provider und Nutzer vereinbart.

Durch De-Mail ergeben sich erhebliche Porto- und Prozesskosteneinsparungen, weil in der Kommunikation mit dem Bürger teure Medienbrüche in erheblichem Ausmaß vermieden werden können. Werden nur 8-9% der Papierpost in der öffentlichen Verwaltung durch De-Mail abgelöst, ergibt sich ein Einsparvolumen von 100 – 150 Mio. EUR pro Jahr.

Zu 29.

Es ist nicht anzunehmen, dass Behörden De-Mails oder elektronische Dokumente in großem Umfang in ihren De-Safes bei De-Mail-Providern speichern werden. Dieser Dienst richtet sich vornehmlich an Bürgerinnen und Bürger bzw. kleinere Organisationen, die selbst eine langfristige und sichere Speicherung nicht gewährleisten können.

Zu 30.

Über die allgemeingültigen Regelungen hinaus wird voraussichtlich eine spezifische Haftungsregelung festgelegt, die derzeit noch abgestimmt wird.

Zu 31.

Die Dokumente im De-Safe werden standardmäßig verschlüsselt abgelegt und nur bei Abruf durch den (authentifizierten) Nutzer durch den De-Mail-Provider entschlüsselt. Durch organisatorische Maßnahmen, die entsprechend zertifiziert werden müssen, wird gewährleistet, dass der Provider nicht unberechtigterweise auf die Daten des Nutzers zugreifen kann. Bei Bedarf kann der Nutzer auch einzelne, alle oder bestimmte Kategorien seiner Dokumente zusätzlich clientseitig verschlüsseln und im De-Safe ablegen.

Zu 32.

Das Vorhaben wird durch gesetzgeberische Schritte begleitet mit dem Ziel, für die potentiellen Diensteanbieter Rechtssicherheit zu schaffen und ihnen zu ermöglichen, die Rechtsqualität der Dienste (gleichbedeutend mit De-Mail-Diensten) im Internet zu steigern. Außerdem sind Änderungen des Zustellrechts geplant.

Zu 33.

Die Konzepte werden den aktuellen Entwicklungen angepasst. Damit werden auch die Zertifizierungskriterien für IT-Sicherheit, Interoperabilität, Datenschutz und Funktionalität regelmäßig aktualisiert.